

JP00/05833

日 本 国 特 許 庁

13.09.00

PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application:

1999年 8月30日

REC'D 06 NOV 2000

WIPO PCT

出 願 番 号
Application Number:

平成11年特許願第243741号

出 願 人
Applicant (s):

富士通株式会社
株式会社日立製作所
日本コロムビア株式会社
三洋電機株式会社

JP 00/05833

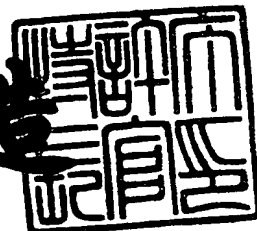
4

PRIORITY
DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

2000年10月20日

特許庁長官
Commissioner,
Patent Office

及 川 耕 造



出証番号 出証特2000-3085322

特平 11-243741

【書類名】	特許願
【整理番号】	1990902
【提出日】	平成11年 8月30日
【あて先】	特許庁長官殿
【国際特許分類】	H04M 11/08
【発明者】	
【住所又は居所】	神奈川県川崎市中原区上小田中4丁目1番1号 富士通
	株式会社内
【氏名】	畑中 正行
【発明者】	
【住所又は居所】	神奈川県川崎市中原区上小田中4丁目1番1号 富士通
	株式会社内
【氏名】	蒲田 順
【発明者】	
【住所又は居所】	神奈川県川崎市中原区上小田中4丁目1番1号 富士通
	株式会社内
【氏名】	畠山 卓久
【発明者】	
【住所又は居所】	神奈川県川崎市中原区上小田中4丁目1番1号 富士通
	株式会社内
【氏名】	長谷部 高行
【発明者】	
【住所又は居所】	神奈川県川崎市中原区上小田中4丁目1番1号 富士通
	株式会社内
【氏名】	小谷 誠剛
【発明者】	
【住所又は居所】	東京都小平市上水本町5丁目20番1号 株式会社日立
	製作所 半導体グループ内
【氏名】	利根川 忠明

【発明者】

【住所又は居所】 東京都港区赤坂四丁目14番14号 日本コロムビア株式会社内

【氏名】 穴澤 健明

【発明者】

【住所又は居所】 大阪府守口市京阪本通2丁目5番5号 三洋電機株式会社内

【氏名】 日置 敏昭

【発明者】

【住所又は居所】 大阪府守口市京阪本通2丁目5番5号 三洋電機株式会社内

【氏名】 金森 美和

【発明者】

【住所又は居所】 大阪府守口市京阪本通2丁目5番5号 三洋電機株式会社内

【氏名】 堀 吉宏

【特許出願人】

【識別番号】 000005223

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号

【氏名又は名称】 富士通株式会社

【特許出願人】

【識別番号】 000005108

【住所又は居所】 東京都千代田区神田駿河台4丁目6番地

【氏名又は名称】 株式会社日立製作所

【特許出願人】

【識別番号】 000004167

【住所又は居所】 東京都港区赤坂四丁目14番14号

【氏名又は名称】 日本コロムビア株式会社

【特許出願人】

【識別番号】 000001889
 【住所又は居所】 大阪府守口市京阪本通 2 丁目 5 番 5 号
 【氏名又は名称】 三洋電機株式会社

【代理人】

【識別番号】 100064746
 【弁理士】
 【氏名又は名称】 深見 久郎

【選任した代理人】

【識別番号】 100085132
 【弁理士】
 【氏名又は名称】 森田 俊雄

【選任した代理人】

【識別番号】 100091409
 【弁理士】
 【氏名又は名称】 伊藤 英彦

【選任した代理人】

【識別番号】 100096781
 【弁理士】
 【氏名又は名称】 堀井 豊

【手数料の表示】

【予納台帳番号】 008693
 【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 記録装置

【特許請求の範囲】

【請求項 1】 暗号化コンテンツデータを再生出力する再生装置に対して着脱可能であって、前記暗号化コンテンツデータを受けて記録するための記録装置であって、

外部との間でデータの授受を可能とするためのデータ入出力部と、

前記データ入出力部からの前記暗号化コンテンツデータを格納するための第 1 の記憶部と、

前記記録装置のユーザを識別するための第 1 のユーザ特定データを保持するためのユーザ情報保持部と、

外部から与えられるユーザ情報と前記第 1 のユーザ特定データとの比較結果に応じて外部からの指示により更新可能な保護情報を保持する保護情報保持部と、

前記記録装置の動作を制御するための制御部とを備え、

前記制御部は、前記保護情報に基づいて、外部からの前記第 1 の記憶部に保持された前記暗号化コンテンツデータに対するアクセスを制限する、記録装置。

【請求項 2】 前記制御部は、外部から与えられるユーザ情報と前記第 1 のユーザ特定データとが一致する場合に、前記ユーザ特定データの変更を可能とする、請求項 1 記載の記録装置。

【請求項 3】 前記制御部は、前記ユーザ情報保持部に前記第 1 のユーザ特定データが未登録の場合に、前記保護情報の変更および前記ユーザ特定データの変更を可能とする、請求項 2 記載の記録装置。

【請求項 4】 前記保護情報保持部は、前記保護情報のうち、前記記録装置自体に対するアクセスの制限に対する第 1 の保守情報を保持する第 1 の保守情報保持部を含み、

前記制御部は、前記第 1 の保守情報に応じて、前記第 1 の記憶部に対して、新たな暗号化コンテンツデータの追記を禁止する、請求項 1 記載の記録装置。

【請求項 5】 前記保護情報保持部は、前記保護情報のうち、前記記録装置自体に対するアクセスの制限に対する第 1

の保守情報を保持する第 1 の保守情報保持部を含み、

前記制御部は、前記第 1 の保守情報に応じて、前記第 1 の記憶部に対して、新たな暗号化コンテンツデータの消去を禁止する、請求項 1 記載の記録装置。

【請求項 6】 前記保護情報保持部は、

前記保護情報のうち、前記暗号化コンテンツデータごとのアクセスの制限に対する第 2 の保守情報を保持する第 2 の保守情報保持部をさらに含み、

前記制御部は、前記第 1 および第 2 の保守情報に応じて、前記第 1 の記憶部に保持され、前記第 2 の保守情報に対応する暗号化コンテンツデータの消去を禁止する、請求項 5 記載の記録装置。

【請求項 7】 前記保護情報保持部は、

前記保護情報のうち、前記暗号化コンテンツデータごとのアクセスの制限に対する第 2 の保守情報を保持する第 2 の保守情報保持部を含み、

前記制御部は、前記第 2 の保守情報に応じて、前記第 1 の記憶部に保持され、前記第 2 の保守情報に対応する暗号化コンテンツデータの消去を禁止する、請求項 1 記載の記録装置。

【請求項 8】 前記制御部は、外部から前記暗号化コンテンツデータの再生動作が指示された場合、前記第 1 の記憶部を制御して、前記第 2 の保守情報に応じて、前記第 1 の記憶部に保持された暗号化コンテンツデータを前記データ入出力部に与えることを禁止する、請求項 6 または 7 記載の記録装置。

【請求項 9】 前記制御部は、外部から与えられるユーザ情報と前記第 1 のユーザ特定データとが一致する場合に、前記第 1 の記憶部を制御して、前記第 2 の保守情報に応じて、前記第 1 の記憶部に保持された暗号化コンテンツデータを前記データ入出力部に与えることを禁止する、請求項 8 記載の記録装置。

【請求項 10】 前記制御部は、前記ユーザ情報保持部に前記第 1 のユーザ特定データが未登録の場合に、前記第 1 の記憶部を制御して、前記第 2 の保守情報に応じて、前記第 1 の記憶部に保持された暗号化コンテンツデータを前記データ入出力部に与えることを禁止する、請求項 8 記載の記録装置。

【請求項 11】 前記制御部は、外部から与えられるユーザ情報と前記第 1 のユーザ特定データとが一致する場合に、前記第 1 および第 2 の保守情報のうち

、少なくとも1つの保守情報を書きかえることを許可する、請求項4～10のいずれか1項に記載の記録装置。

【請求項12】 前記制御部は、前記ユーザ情報保持部に前記第1のユーザ特定データが未登録の場合に、前記第1および第2の保守情報のうち、少なくとも1つの保守情報を書きかえることを許可する、請求項4～10のいずれか1項に記載の記録装置。

【請求項13】 前記記録装置は、

前記暗号化コンテンツデータにそれぞれ対応し、前記暗号化コンテンツデータを再生するために必要なライセンス情報データを保持するための第2の記憶部をさらに備え、

前記制御部は、外部から前記第1の記憶部に保持された前記暗号化コンテンツデータの移動が指示された場合、外部から与えられる前記再生装置に対する第2のユーザ特定データと、前記ユーザ情報保持部に保持される前記第1のユーザ特定データとの比較結果に応じて、前記第2の記憶部を制御して、前記ライセンス情報データを前記データ入出力部に与える、請求項1記載の記録装置。

【請求項14】 前記記録装置は、

前記暗号化コンテンツデータにそれぞれ対応し、前記暗号化コンテンツデータを再生するために必要なライセンス情報データを保持するための第2の記憶部をさらに備え、

前記ライセンス情報の各々は、前記暗号化コンテンツデータごとに対応するコンテンツユーザ特定データを含み、

前記制御部は、外部から前記第1の記憶部に保持された前記暗号化コンテンツデータの移動が指示された場合、外部から与えられる前記再生装置に対する第2のユーザ特定データと、前記ユーザ情報保持部に保持される前記第1のユーザ特定データと、前記コンテンツユーザ特定データとの比較結果に応じて、前記第2の記憶部を制御して、前記暗号化コンテンツデータごとに前記ライセンス情報データを前記データ入出力部に与える、請求項1記載の記録装置。

【請求項15】 前記コンテンツユーザ特定データは、対応する前記暗号化コンテンツデータの配信の際に前記ユーザ情報保持部に保持される前記第1のユ

ーザ特定データである、請求項 1 4 記載の記録装置。

【請求項 1 6】 前記制御部は、外部から与えられる前記再生装置に対する第 2 のユーザ特定データと、前記ユーザ情報保持部に保持される前記第 1 のユーザ特定データとの比較結果に応じて、前記コンテンツユーザ特定データの変更を許可する、請求項 1 4 または 1 5 記載の記録装置。

【請求項 1 7】 前記第 1 の記憶部は、半導体メモリであり、

前記記録装置は、メモリカードである、請求項 1 ～ 1 6 のいずれか 1 項に記載の記録装置。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、携帯電話機等の端末に対して暗号化して配信された情報を格納して保持するための、メモリカードなどの記録媒体として機能する記録装置の構成に関するものである。

【0 0 0 2】

【従来の技術】

近年、インターネット等の情報通信網等の進歩により、携帯電話等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【0 0 0 3】

このような情報通信においてはデジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像情報を各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、情報のコピーを行なうことが可能である。

【0 0 0 4】

したがって、このような情報通信網上において、音楽情報や画像情報等の著作権の存在する創作物が伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【0 0 0 5】

一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物情報の配信を行なうことができないとすると、基本的には、著作物の複製に際して一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【0006】

【発明が解決しようとする課題】

ところで、上述したようなデジタル情報通信網を介した音楽データなどの著作物情報の配信が行なわれた場合、各ユーザは、このようにして配信されたコンテンツデータを何らかの記録媒体に記録して保持することになる。

【0007】

このような記録媒体としては、たとえばメモリカードのように電氣的にデータの書込および消去が可能な媒体が用いられることになる。

【0008】

この場合、著作権者の承諾なしに、このようにして配信を受けたコンテンツデータ（音楽データ等）を自由に当該記録媒体から他の記録媒体等へ移転できるものとする、著作権者の権利保護が図れない。

【0009】

それのみならず、このようにして正当な対価を支払った上でコンテンツデータの配信を受けたユーザ以外のものが、当該記録媒体から音楽データ等の再生を行なったり、コンテンツデータの移動や消去を自由に行なえることとすると、ユーザ側の権利保護にも支障を来すことになる。

【0010】

本発明は、上記のような問題点を解決するためになされたものであって、その目的は、音楽データ等の著作物データを格納した記録媒体に保持されたコンテンツデータに対して、ユーザ以外の者が無断で再生、移転消去等を行なうことから保護する機能を備えたデータの記録媒体として機能する記録装置を提供することである。

【0011】

【課題を解決するための手段】

請求項 1 記載の記録装置は、暗号化コンテンツデータを再生出力する再生装置に対して着脱可能であって、暗号化コンテンツデータを受けて記録するための記録装置であって、外部との間でデータの授受を可能とするためのデータ入出力部と、データ入出力部からの暗号化コンテンツデータを格納するための第 1 の記憶部と、記録装置のユーザを識別するための第 1 のユーザ特定データを保持するためのユーザ情報保持部と、外部から与えられるユーザ情報と第 1 のユーザ特定データとの比較結果に応じて外部からの指示により更新可能な保護情報を保持する保護情報保持部と、記録装置の動作を制御するための制御部とを備え、制御部は、保護情報に基づいて、外部からの第 1 の記憶部に保持された暗号化コンテンツデータに対するアクセスを制限する。

【0012】

請求項 2 記載の記録装置は、請求項 1 記載の記録装置の構成に加えて、制御部は、外部から与えられるユーザ情報と第 1 のユーザ特定データとが一致する場合に、ユーザ特定データの変更を可能とする。

【0013】

請求項 3 記載の記録装置は、請求項 2 記載の記録装置の構成に加えて、制御部は、ユーザ情報保持部に第 1 のユーザ特定データが未登録の場合に、保護情報の変更およびユーザ特定データの変更を可能とする。

【0014】

請求項 4 記載の記録装置は、請求項 1 記載の記録装置の構成に加えて、保護情報保持部は、保護情報のうち、記録装置自体に対するアクセスの制限に対する第 1 の保守情報を保持する第 1 の保守情報保持部を含み、制御部は、第 1 の保守情報に応じて、第 1 の記憶部に対して、新たな暗号化コンテンツデータの追記を禁止する。

【0015】

請求項 5 記載の記録装置は、請求項 1 記載の記録装置の構成に加えて、保護情報保持部は、保護情報のうち、記録装置自体に対するアクセスの制限に対する第 1 の保守情報を保持する第 1 の保守情報保持部を含み、制御部は、第 1 の保守情報に応じて、第 1 の記憶部に対して、新たな暗号化コンテンツデータの消去を禁

止する。

【0016】

請求項6記載の記録装置は、請求項5記載の記録装置の構成に加えて、保護情報保持部は、保護情報のうち、暗号化コンテンツデータごとのアクセスの制限に対する第2の保守情報を保持する第2の保守情報保持部をさらに含み、制御部は、第1および第2の保守情報に応じて、第1の記憶部に保持され、第2の保守情報に対応する暗号化コンテンツデータの消去を禁止する。

【0017】

請求項7記載の記録装置は、請求項1記載の記録装置の構成に加えて、保護情報保持部は、保護情報のうち、暗号化コンテンツデータごとのアクセスの制限に対する第2の保守情報を保持する第2の保守情報保持部を含み、制御部は、第2の保守情報に応じて、第1の記憶部に保持され、第2の保守情報に対応する暗号化コンテンツデータの消去を禁止する。

【0018】

請求項8記載の記録装置は、請求項6または7記載の記録装置の構成に加えて、制御部は、外部から暗号化コンテンツデータの再生動作が指示された場合、第1の記憶部を制御して、第2の保守情報に応じて、第1の記憶部に保持された暗号化コンテンツデータをデータ入出力部に与えることを禁止する。

【0019】

請求項9記載の記録装置は、請求項8記載の記録装置の構成に加えて、制御部は、外部から与えられるユーザ情報と第1のユーザ特定データとが一致する場合に、第1の記憶部を制御して、第2の保守情報に応じて、第1の記憶部に保持された暗号化コンテンツデータをデータ入出力部に与えることを禁止する。

【0020】

請求項10記載の記録装置は、請求項8記載の記録装置の構成に加えて、制御部は、ユーザ情報保持部に第1のユーザ特定データが未登録の場合に、第1の記憶部を制御して、第2の保守情報に応じて、第1の記憶部に保持された暗号化コンテンツデータをデータ入出力部に与えることを禁止する。

【0021】

請求項 11 記載の記録装置は、請求項 4～10 のいずれか 1 項に記載の記録装置の構成に加えて、制御部は、外部から与えられるユーザ情報と第 1 のユーザ特定データとが一致する場合に、第 1 および第 2 の保守情報のうち、少なくとも 1 つの保守情報を書きかえることを許可する。

【0022】

請求項 12 記載の記録装置は、請求項 4～10 のいずれか 1 項に記載の記録装置の構成に加えて、制御部は、ユーザ情報保持部に第 1 のユーザ特定データが未登録の場合に、第 1 および第 2 の保守情報のうち、少なくとも 1 つの保守情報を書きかえることを許可する。

【0023】

請求項 13 記載の記録装置は、請求項 1 に記載の記録装置の構成に加えて、記録装置は、暗号化コンテンツデータにそれぞれ対応し、暗号化コンテンツデータを再生するために必要なライセンス情報データを保持するための第 2 の記憶部をさらに備え、制御部は、外部から第 1 の記憶部に保持された暗号化コンテンツデータの移動が指示された場合、外部から与えられる再生装置に対する第 2 のユーザ特定データと、ユーザ情報保持部に保持される第 1 のユーザ特定データとの比較結果に応じて、第 2 の記憶部を制御して、ライセンス情報データをデータ入出力部に与える。

【0024】

請求項 14 記載の記録装置は、請求項 1 に記載の記録装置の構成に加えて、記録装置は、暗号化コンテンツデータにそれぞれ対応し、暗号化コンテンツデータを再生するために必要なライセンス情報データを保持するための第 2 の記憶部をさらに備え、ライセンス情報の各々は、暗号化コンテンツデータごとに対応するコンテンツユーザ特定データを含み、制御部は、外部から第 1 の記憶部に保持された暗号化コンテンツデータの移動が指示された場合、外部から与えられる再生装置に対する第 2 のユーザ特定データと、ユーザ情報保持部に保持される第 1 のユーザ特定データと、コンテンツユーザ特定データとの比較結果に応じて、第 2 の記憶部を制御して、暗号化コンテンツデータごとにライセンス情報データをデータ入出力部に与える。

【0025】

請求項15記載の記録装置は、請求項14に記載の記録装置の構成に加えて、コンテンツユーザ特定データは、対応する暗号化コンテンツデータの配信の際にユーザ情報保持部に保持される第1のユーザ特定データである。

【0026】

請求項16記載の記録装置は、請求項14または15に記載の記録装置の構成に加えて、制御部は、外部から与えられる再生装置に対する第2のユーザ特定データと、ユーザ情報保持部に保持される第1のユーザ特定データとの比較結果に応じて、コンテンツユーザ特定データの変更を許可する。

【0027】

請求項17記載の記録装置は、請求項1から16のいずれか1項に記載の記録装置の構成に加えて、第1の記憶部は、半導体メモリであり、記録装置は、メモリカードである。

【0028】

【発明の実施の形態】

〔実施の形態1〕

〔配信データの受信端末（携帯電話）の構成〕

図1は、本発明の記録媒体が使用される情報配信システムにおいて、情報の配信を受けるための端末である携帯電話機100の構成を説明するための概略ブロック図である。

【0029】

図1を参照して、携帯電話機100は、携帯電話網により無線伝送される信号を受信するためのアンテナ1102と、アンテナ1102からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機100からのデータを変調してアンテナ1102に与えるための送受信部1104と、携帯電話機100の各部のデータ授受を行なうためのデータバスBS2と、データバスBS2を介して携帯電話機100の動作を制御するためのコントローラ1106と、携帯電話機100の所有者を識別するためのユーザIDデータUser-IDhを保持するユーザID保持部1107と、外部からの指示を携帯電話機100に与えるためのタ

タッチキー部 1108 と、コントローラ 1106 から出力される情報をユーザに視覚情報として与えるためのディスプレイ 1110 と、通常の通話動作において、データバス BS2 を介して与えられる受信データに基づいて音声を再生するための音声再生部 1112 と、外部との間でデータの授受を行なうためのコネクタ 1120 と、コネクタ 1120 からのデータをデータバス BS2 に与え得る信号に変換し、または、データバス BS2 からのデータをコネクタ 1120 に与え得る信号に変換するための外部インターフェイス部 1122 とを備える。

【0030】

ここで、たとえば、ユーザ ID データは、ユーザの携帯電話機の電話番号、またはユーザ自身が設定したデータ、あるいはその両者の組合せのデータ等を含む。

【0031】

携帯電話機 100 は、さらに、音楽サーバから供給される暗号化コンテンツデータを格納するための着脱可能なメモリカード 110 と、メモリカード 110 とデータバス BS2 との間のデータの授受を制御するためのメモリインターフェイス 1200 と、メモリカード 110 からの暗号化されたコンテンツデータとこの暗号化されたコンテンツデータを復号するためのコンテンツキー Kc とを受けて、音楽データを再生するための音楽再生部 1508 と、音楽再生部 1508 の出力と音声再生部 1112 の出力とを受けて、動作モードに応じて選択的に出力するための混合部 1510 と、混合部 1510 の出力を受けて、外部に出力するためのアナログ信号に変換するデジタルアナログ変換部 1512 と、デジタルアナログ変換部 1512 の出力を受けて、たとえば、ヘッドホーン（図示せず）と接続するための接続端子 1514 とを含む。

【0032】

なお、説明の簡略化のため本発明の記録媒体中に格納された音楽データの配信および再生に係るブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、図 1 では一部割愛されている。

【0033】

〔メモリカードの構成〕

図2は、図1に示したメモリカード110の構成を説明するための概略ブロック図である。

【0034】

以下では、携帯電話機100に装着されるメモリカード110に固有な秘密復号キーをキー $K_{mc}(1)$ とする。一方、他のメモリカードに固有な秘密復号キーをキー $K_{mc}(n)$ (n :自然数)とする。ここで、自然数 n は、メモリカードを区別するためのものである。すなわち、キー $K_{mc}(n)$ は、メモリカードごとに異なるものである。

【0035】

また、これに対応して、秘密復号キー $K_{mc}(1)$ で復号可能な暗号化を提供し、キー $K_{mc}(1)$ とは非対称な、言い換えると同一の秘密復号キー $K_{mc}(1)$ に対して複数個存在し得る公開暗号化キーを公開暗号化キー $KP_{mc}(1)$ と称し、同様に、秘密復号キー $K_{mc}(n)$ で復号可能な暗号化を提供し、キー $K_{mc}(n)$ とは非対称な公開暗号化キーを公開暗号化キー $KP_{mc}(n)$ と称することとする。

【0036】

図2を参照して、メモリカード110は、インターフェイス1200との間で信号を端子1202を介して授受するデータバスBS3と、公開暗号化キー $KP_{mc}(1)$ を保持し、データバスBS3に公開暗号化キー $KP_{mc}(1)$ を出力するための $KP_{mc}(1)$ 保持部1405と、端子1202およびデータバスBS3を介して他のメモリカードから送信された公開暗号化キー $KP_{mc}(n)$ に基づいて、入力されたデータを暗号化するための暗号化処理部1414と、秘密復号キー $K_{mc}(1)$ を保持するための $K_{mc}(1)$ 保持部1415と、データバスBS3から与えられるデータを受けて、 $K_{mc}(1)$ 保持部1415からの秘密復号キー $K_{mc}(1)$ に基づいて復号処理をするための復号処理部1416と、メモリカード110の動作を制御するためのコントローラ1420と、データバスBS3を介して、配信される暗号化コンテンツデータ $[Dc(i)]Kc(i)$ と、暗号化されたコンテンツキーおよびライセンス情報データ $[Kc(i), License(i)]K_{mc}(1)$ を格納し保持するためのメモリ141

2とを含む。メモリ1412は、いわゆる半導体メモリであって、とくに限定されないが、たとえば、不揮発性メモリであるフラッシュメモリ等を用いることが可能である。

【0037】

ここで、記号[X] Yは、復号キーYで復号可能な暗号化処理でデータXが暗号化されていることを表わす。

【0038】

メモリカード110は、さらに、メモリカード110についてのユーザに関する情報であるユーザIDデータを保持するためのユーザID保持部1530と、メモリカード110に対する保守情報を保持するための第1の保守情報保持部1520と、復号処理部1416から出力される復号化されたデータを暗号化処理部1414およびコントロール1420等へ伝達するためのデータバスBS5と、コンテンツデータDc(i)に対応し、当該コンテンツデータの再生回数の制限等の再生権に関する情報やコンテンツデータの所有権等を示すライセンス情報データLicense(i)を保持するためのライセンス情報保持部1500と、コンテンツデータDc(i) (i:自然数)ごとに設定されるコンテンツ保守情報を保持するための第2の保守情報保持部1540とを備える。

【0039】

なお、上述した構成において、コンテンツデータDc(i)やコンテンツキーデータKc(i)、ライセンス情報データLicense(i)等の自然数iは、各コンテンツデータごとにこれらのデータが異なることを表現している。

【0040】

また、図2において実線で囲んだ領域は、メモリカード110内において、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールTRMに組込まれているものとする。

【0041】

このようなモジュールは、一般にはタンパーレジスタンスモジュール (Tamper Resistance Module) と呼ばれる。

【0042】

もちろん、メモリ1412も含めて、モジュールTRMに組込まれる構成としてもよい。しかしながら、図2に示したような構成とすることで、メモリ1412中に保持されているデータは、いずれも暗号化されているデータであるため、第三者はこのメモリ1412中のデータのみでは、音楽データ等のコンテンツデータを再生することは不可能である。このため、高価なタンパーレジスタンスモジュール内にメモリ1412を設ける必要がないので、製造コストが低減されるという利点がある。

【0043】

ここで、メモリカード110に対する動作として、メモリ1412中に保持されているコンテンツデータをそのままの状態に保持して、さらに異なるコンテンツデータを追加して記録する動作を「追記」と呼び、メモリ1412中に含まれるコンテンツデータ等を消去する動作または再生できる状態にする動作を「消去」と呼ぶ。

【0044】

以下の表1は、図2に示した第1の保守情報保持部1520中に保持される上記追記動作および消去動作を制御するための追記フラグおよびメディア消去フラグの状態と、それに対応するメモリカードの動作状態との関係を説明する表である。

【0045】

【表1】

メディア単位の管理

保守情報 \ 値	1	0
追記フラグ	追記可能	追記禁止
メディア消去フラグ	消去可能	消去禁止

【0046】

すなわち、第1の保守情報保持部1520中に保持される追記フラグが「1」である場合は、メモリ1412中に保持されたコンテンツデータに加えて、さらに新たなコンテンツデータの書込を行なうことが許可されており、追記フラグが「0」である場合はこのような追記動作が禁止されている。

【0047】

一方、第1の保守情報保持部1520に保持されるメディア消去フラグが「1」である場合は、このメモリカード110に対してメモリ1412に保持されたデータを外部からの指示に応じて消去することが可能であるのに対し、メディア消去フラグが「0」である場合はこのような消去動作は一切禁止されている。

【0048】

一方、メモリカード110は、外部から与えられる指示に応じて、コントローラ1420の制御の下、メモリ1412中に保持された各コンテンツデータごとの処理を制御するための保守情報を第2の保守情報保持部1540が保持している。

【0049】

以下では、コンテンツデータごとの再生処理を特に「コンテンツ再生」と呼び、コンテンツデータごとの消去動作を特に「コンテンツ消去」と呼ぶことにする。

【0050】

表2は、第2の保守情報保持部1540が保持するデータと、メモリカード110のコントローラ1420による制御状態との関係を示す表である。

【0051】

【表 2】

コンテンツデータ単位の管理		
保守情報 \ 値	1	0
コンテンツ再生フラグ	再生可能	再生禁止*
コンテンツ消去フラグ	消去可能	消去禁止

*) 携帯電話機におけるユーザIDが同一の場合は再生可能

【0052】

すなわち、第2の保守情報保持部1540が各コンテンツデータごとに対応して保持するコンテンツ再生フラグが「1」である場合は、対応するコンテンツデータは再生可能状態であり、コンテンツ再生フラグが「0」である場合は原則として当該コンテンツデータの再生は禁止される。

【0053】

ただし、以下に説明するようにコンテンツ再生フラグが「0」である場合であっても、携帯電話機100のユーザIDデータとメモリカードのユーザIDデータとが一致する場合は、当該コンテンツデータの再生動作が許可される。

【0054】

一方、第2の保守情報保持部1540においてコンテンツデータごとに対応して保持されるコンテンツ消去フラグが「1」である場合は、当該コンテンツデータに関しては消去動作が許可されており、コンテンツ消去フラグが「0」である場合は当該コンテンツデータに対する消去動作が禁止されている。

【0055】

以上のように、メモリカードごとおよびコンテンツデータごとに予め保守情報を設定しておくことで、正規ユーザ以外の者がメモリカード110内に保持されたコンテンツデータに対する処理を行なうことを制限し、当該メモリカードのユーザが正当な対価の下に購入したコンテンツデータを保護することが可能となる。

【0056】

〔配信システムの全体構成〕

図3は、本発明の記録媒体が用いられる情報配信システムの全体構成を概略的に説明するための概念図である。

【0057】

なお、以下では携帯電話網を介して、デジタル音楽データを各ユーザに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物情報データ、たとえば画像データ等の著作物データを、メモリ等に配信した上でアクセスするあらゆる場合にも適用することが可能なものである。

【0058】

また、データの配信の方法も携帯電話網による配信に限られるものではなく、たとえば、他の情報通信網を介した配信や、多数のコンテンツデータを蓄えたコンテンツデータ販売機を街頭に設置し、ユーザは、携帯電話機のインターフェースを介して、または、メモリカードに直接にこのコンテンツデータ販売機からコンテンツデータを購入することで、著作物データを入手する構成としても良い。

【0059】

さらに、暗号化されたコンテンツデータを再生する機器も、携帯電話機に限定されることなく、たとえば、上記メモリカードに対応した専用の再生装置であってもよい。

【0060】

図3を参照して、著作権の存在する音楽情報を管理する配信サーバ10は、所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化したうえで、音楽データを配信するための配信キャリアである携帯電話会社20に、このような暗号化コンテンツデータを与える。一方、認証サーバ12は、音楽データの配信を求めてアクセスしてきたユーザが正規のユーザであるか否かの認証を行う。

【0061】

携帯電話会社20は、自己の携帯電話網を通じて、各ユーザからの配信要求（

配信リクエスト)を配信サーバ10に中継する。配信サーバ10は、配線リクエストがあると、認証サーバ12によりユーザが正規のユーザであることを確認し、要求された音楽情報をさらに暗号化したうえで、携帯電話会社20の携帯電話網を介して、各ユーザの携帯電話機に対してコンテンツデータを配信する。

【0062】

図3においては、たとえば、携帯電話ユーザ1の携帯電話機100には、携帯電話機100により受信された暗号化された音楽データを受取って、上記送信にあたって行なわれた暗号化については復号化したうえで、携帯電話機100中の音楽再生部(図示せず)に与えるために、図2において説明したような着脱可能なメモリカード110が装着される構成となっている。

【0063】

さらに、たとえばユーザ1は、携帯電話機100に接続したヘッドホン120等を介してこのような再生された音楽データを聴取することが可能である。

【0064】

以下では、このような配信サーバ10と認証サーバ12と配信キャリア(携帯電話会社)20とを併せて、音楽サーバ30と総称することにする。

【0065】

また、このような音楽サーバ30から、各携帯電話端末等に音楽情報を伝送する処理を「配信」と称することとする。

【0066】

このような構成とすることで、まず、メモリカード110を購入していない正規のユーザでないものは、音楽サーバ30からの配信データを受取って再生することが困難な構成となる。

【0067】

しかも、配信キャリア20において、たとえば1曲分の音楽データを配信するたびにその度数を計数しておくことで、ユーザが著作物データを受信するたびに発生する著作権料を、配信キャリア20が携帯電話の通話料金として徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【0068】

しかも、このような著作物データの配信は、携帯電話網というクローズドなシステムを介して行なわれるため、インターネット等のオープンなシステムに比べて、著作権保護の対策を講じやすいという利点がある。

【0069】

このとき、たとえばメモリカード112を有するユーザ2が、自己の携帯電話機102により、音楽サーバ30から直接音楽データの配信を受けることは可能である。しかしながら、相当量の情報量を有する音楽データ等をユーザ2が直接音楽サーバ30から受信することとすると、その受信のために比較的長い時間を要してしまう場合がある。このような場合、既に当該音楽データの配信を受けているユーザ1から、その音楽情報をコピーできることを可能としておけば、ユーザ2にとっての利便性が向上する。

【0070】

図3に示した例では、ユーザ1が受信した音楽データを、デジタル音楽データそのものおよび当該音楽データを再生可能とするために必要な情報とともに、ユーザ2に対してコピーさせる場合を音楽データの「移動」と呼ぶ。この場合、ユーザ1は、再生のために必要な情報（再生情報）ごとユーザ2にコピーさせるため、情報の移動を行なった後には、ユーザ1においては音楽データの再生を行なうことを不可能とする必要がある。ここで、「再生情報」とは、後に説明するように、上記所定の暗号化方式に従って暗号化されたコンテンツデータを復号可能なコンテンツキーと、著作権保護に関わる情報であるライセンスIDデータやユーザIDデータ等のライセンス情報とを意味する。

【0071】

これに対して、音楽データ（コンテンツデータ）のみを暗号化されたままの状態、ユーザ2にコピーさせることを音楽情報の「複製」と呼ぶこととする。

【0072】

この場合、ユーザ2の端末には、このようなコンテンツデータを再生させるために必要な再生情報はコピーされないため、ユーザ2は、コンテンツデータを得ただけでは、音楽情報を再生させることができない。したがって、ユーザ2が、このような音楽情報の再生を望む場合は、改めて音楽サーバ30からコンテンツ

データの再生を可能とするための再生情報の配信を受ける必要がある。しかしながら、この場合は、再生を可能とするための情報の配信のみを受ければよいので、ユーザ2が直接音楽サーバ30からすべての情報の配信を受ける場合に比べて、格段に短い通話時間で、音楽再生を可能とすることができる。

【0073】

たとえば、携帯電話機100および102が、PHS (Personal Handy Phone) である場合には、いわゆるトランシーバモードの通話が可能となっているので、このような機能を利用して、ユーザ1からユーザ2への一括した情報の移転（移動）や、コンテンツデータのみの転送（複製）を行なうことが可能である。

【0074】

〔暗号／復号キーの構成〕

図4は、図3に示した情報配信システムにおいて使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

【0075】

まず、図3に示した構成において、メモ리카ード110内のデータ処理を管理するための鍵としては、メモ리카ードごとに異なる公開暗号化鍵 $K_{Pmc}(n)$ と、公開暗号化鍵 $K_{Pmc}(n)$ により暗号化されたデータを復号するための秘密復号鍵 $K_{mc}(n)$ とがある。

【0076】

ここで、鍵 $K_{mc}(n)$ や鍵 $K_{Pmc}(n)$ の表記中の自然数 n は、各メモ리카ードを区別するための番号を表わす。

【0077】

したがって、メモ리카ードにおける配信データの授受にあたっては、後に説明するように2つの暗号鍵 $K_{mc}(n)$ 、 $K_{Pmc}(n)$ が用いられることになる。

【0078】

また、メモ리카ードは、メモ리카ードのユーザを識別するためのユーザIDデータ $User-ID_m$ を保持している。一方、携帯電話は、携帯電話機のユーザを識別するためのユーザIDデータ $User-ID_h$ を保持している。

【0079】

さらに、配信されるべきデータについては、まず、音楽データ（コンテンツデータ）自体を暗号化するための共通鍵であるKc（以下、ライセンスキーと呼ぶ）があり、この共通鍵Kcにより暗号化されたコンテンツデータが復号化されるものとする。さらに、上述したライセンス情報として、当該コンテンツデータを特定できる管理コードや、再生を行なう回数の制限などの情報を含むライセンス情報データLicense(i)等が存在する。

【0080】

このような構成とすることで、ライセンスIDデータに含まれる情報に応じて、著作権者側の著作権保護に関する制御を行なうことが可能であり、一方ユーザIDデータを用いることで、コンテンツデータの配信を正規に受けたユーザの保護、たとえば、ユーザの許可無く、配信されたコンテンツデータが消去されることを防止するなどの制御を行なうことが可能である。

【0081】

配信データにおけるコンテンツデータDcは、上述のとおり、たとえば音楽情報データであり、このコンテンツデータをライセンスキーKcで復号化可能なデータを、暗号化コンテンツデータ[Dc]Kcと呼ぶ。

【0082】

[配信サーバ10の構成]

図5は、図3に示した配信サーバ10の構成を示す概略ブロック図である。

【0083】

配信サーバ10は、音楽データ（コンテンツデータ）を所定の方式に従って暗号化したデータや、ライセンスIDデータ等の配信情報を保持するための配信情報データベース304と、各ユーザごとに音楽情報へのアクセス回数等に従った課金情報を保持するための課金データベース302と、配信情報データベース304および課金データベース302からのデータをデータバスBS1を介して受取り、所定の暗号化処理を行なうためのデータ処理部310と、通信網を介して、配信キャリア20とデータ処理部310との間でデータ授受を行なうための通信装置350とを備える。

【 0 0 8 4 】

データ処理部 3 1 0 は、データバス B S 1 上のデータに応じて、データ処理部 3 1 0 の動作を制御するための配信制御部 3 1 2 と、携帯電話通信網を介して、通信装置 3 5 0 により受信されたメモリカード n からの公開暗号化キー K P m c (n) を受取り、配信制御部 3 1 2 から与えられる暗号化コンテンツデータを、この公開暗号化キー K P m c (n) で更に暗号化してデータバス B s 1 に与えるための暗号化処理部 3 2 0 とを備える。

【 0 0 8 5 】

通信装置 3 5 0 は、このようにして暗号化処理部 3 2 0 により暗号化されたコンテンツデータを後に説明するように通信網と、配信キャリア 2 0 と、携帯電話網とを介して携帯電話機端末 1 0 0 等に送信する。

【 0 0 8 6 】

〔実施の形態 1 の配信処理（保守情報がない場合）〕

図 6 は、図 1、図 2、図 3 および図 5 で説明した情報配信システムにおけるコンテンツデータの配信動作を説明するためのフローチャートである。

【 0 0 8 7 】

図 6 においては、ユーザ 1 が、メモリカード 1 1 0 を用いることで、音楽サーバ 3 0 から音楽データの配信を受ける場合の動作を説明している。

【 0 0 8 8 】

まず、配信動作が開始されると、ユーザ 1 の携帯電話機 1 0 0 からユーザによりキーボード 1 1 0 8 のキーボタンの操作等によって、配信リクエストがなされる（ステップ S 1 0 0）。

【 0 0 8 9 】

配信サーバ 3 0 は、携帯電話機 1 0 0 からの配信リクエストを受理すると、携帯電話機 1 0 0 に対して、公開暗号化キー K P m c (1) の送信要求を出力する（ステップ S 1 0 2）。

【 0 0 9 0 】

携帯電話機 1 0 0 は、サーバ 3 0 からの公開暗号化キー K P m c (1) の送信要求を受信すると（ステップ S 1 0 4）、カード 1 1 0 に対して転送し、カード

110は、これに応じて、公開暗号化キー $KP_{mc}(1)$ を携帯電話機100に対して出力する（ステップS106）。

【0091】

携帯電話機100は、メモ리카ード110からのキーデータ $KP_{mc}(1)$ を受けると、サーバ30に対してこれを送信する（ステップS108）。

【0092】

配信サーバ10は、携帯電話機100からのキー $KP_{mc}(1)$ を受信すると（ステップS110）、配信情報データベース304からの情報をもとにライセンス情報データ $License$ を生成する（ステップS112）。

【0093】

続いて、配信サーバ30は、配信情報データベース304から、コンテンツキー Kc により暗号化されている暗号化コンテンツデータ $[Dc]Kc$ を取得する（ステップS114）。

【0094】

続いて配信サーバ30は、携帯電話機100へ暗号化コンテンツデータ $[Dc]Kc$ を送信する（ステップS116）。

【0095】

携帯電話機100は、暗号化コンテンツデータ $[Dc]Kc$ を受信すると（ステップS118）、メモ리카ード110に転送し、メモ리카ード110は、暗号化コンテンツデータ $[Dc]Kc$ をメモリ1412にそのまま格納する（ステップS120）。

【0096】

一方、サーバ30は、コンテンツキー Kc を配信情報データベースより取得し（ステップS122）、メモ리카ード110から送信された公開暗号化キー $KP_{mc}(1)$ によりこのコンテンツキー Kc およびライセンス情報データ $License$ を暗号化して、データ $[Kc, License]K_{mc}(1)$ を生成する（ステップS124）。

【0097】

配信サーバ10から携帯電話機100へデータ [Kc, License] Kmc (1) が送信され (ステップS126)、携帯電話機100がこれを受信すると (ステップS128)、メモリカード110は携帯電話機100からこのデータ [Kc, License] Kmc (1) を受取ってメモリ1412に格納する (ステップS130)。

【0098】

続いて、メモリカード110は、秘密復号キーKmc (1) によりデータ [Kc, License] Kmc (1) を復号し、抽出されたライセンスデータLicenseをライセンス情報保持部1500に格納する (ステップS132)。

【0099】

ライセンス情報データLicenseのライセンス情報保持部1500への格納の終了に応じて、携帯電話機100から配信サーバ30に対して配信受理が送信される (ステップS134)。

【0100】

サーバ30は配信受理を受信すると (ステップS136)、課金データベースに配信情報を記録する (ステップS138)。

【0101】

以上のような処理により、サーバ30からメモリカード110に対してコンテンツデータ、ライセンス情報データLicenseおよびコンテンツキーKcが配信される。

【0102】

〔実施の形態1の再生処理 (保守情報による保護のない場合) 〕

図7は、携帯電話機100内において、メモリカード110に保持された暗号化コンテンツデータから、音楽データを復号化し、音楽として外部に出力するための再生処理を説明するためのフローチャートである。以下の説明では、まず、上述したような保守情報により再生処理に保護がかかっていない状態の処理のフローを説明する。

【0103】

なお、以下では、暗号化されたデータを復号化した状態、すなわち、本来の状

態に復帰したデータを「平文データ」と呼ぶことにする。

【0104】

図7を参照して、再生処理が開始されると、まず携帯電話機100のキーボード1108等からユーザ1の指示により、再生リクエストがメモリカード110に対して出力される（ステップS200）。

【0105】

カード110においては、この再生リクエストに応じて、コントローラ1420は、ライセンス情報保持部1500に保持されるライセンス情報データに基づいて、復号可能なデータに対するリクエストであるかを判断し（ステップS202）、再生可能と判断した場合はメモリ1412内のライセンス情報データ[Kc, License] Kmc(1)を秘密復号キーKmc(1)により復号する（ステップS204）。

【0106】

一方、コントローラ1420が再生不可能と判断した場合は、処理が終了する（ステップS216）。

【0107】

再生可能と判断され、カード110において、メモリ1412内のデータ[Kc, License] Kmc(1)が復号処理されることで、コンテンツキーKcが抽出されると（ステップS204）、カード110からコンテンツキーKcが携帯電話機100に対して出力される（ステップS206）。

【0108】

携帯電話機100が、コンテンツキーKcを受理すると（ステップS208）、続いて、メモリカード110からはメモリ1412内の暗号化コンテンツデータ[Dc] kcが携帯電話機100に対して出力される（ステップS210）。

【0109】

携帯電話機100においては、音楽再生部1508が、メモリカード110から与えられたコンテンツキーKcにより暗号化コンテンツデータ[Dc] Kcを復号処理して、平文化された音楽データを生成する（ステップS212）。

【0110】

音楽再生部 1 5 0 8 からの出力は混合部 1 5 1 0 を経由して、デジタルアナログ変換処理部 1 5 1 2 に伝達され、デジタルアナログ変換処理部 1 5 1 2 から平文化音楽データがアナログ音楽信号として再生出力されて（ステップ S 2 1 4）、再生処理が終了する（ステップ S 2 1 6）。

【0 1 1 1】

以上の処理により、配信サーバ 1 0 からメモリカード 1 1 0 に対して配信された暗号化コンテンツキーに基づいて、音楽の再生処理が行なわれることになる。

【0 1 1 2】

〔実施の形態 1 の移動処理（保守情報による保護のない場合）〕

図 8 および図 9 は、2 つのメモリカード間において、コンテンツデータおよびキーデータの移動を行なう処理を説明するためのフローチャートである。

【0 1 1 3】

また、図 8 および図 9 においても、まず、保守情報による保護がない場合について説明する。

【0 1 1 4】

まず、携帯電話機 1 0 2 が送信側であり、携帯電話機 1 0 0 が受信側であるものとする。また、携帯電話機 1 0 2 にも、メモリカード 1 1 0 と同様の構成を有するメモリカード 1 1 2 が装着されているものとする。

【0 1 1 5】

移動動作が開始されると、携帯電話機 1 0 2 におけるキータッチ部 1 1 0 8 等とから、ユーザ 2 により移動リクエストが指示され（ステップ S 3 0 0）、携帯電話機 1 0 2 から携帯電話機 1 0 0 へ公開暗号化キー K P m c (1) の送信要求が送信される（ステップ S 3 0 2）。

【0 1 1 6】

携帯電話機 1 0 0 が公開暗号化キー K P m c (1) の送信要求を受信すると（ステップ S 3 0 4）、メモリカード 1 1 0 は、これに応じて、公開暗号化キー K P m c (1) を出力する（ステップ S 3 0 6）。

【0 1 1 7】

携帯電話機 1 0 0 は、メモリカード 1 1 0 からの公開暗号化キー K P m c (1)

）を受取って携帯電話機 102 に対して出力し（ステップ S308）、携帯電話機 102 は、キー K P m c (1) を受信すると（ステップ S310）、これをメモリカード 112 に転送する。

【0118】

メモリカード 112 は、キーデータ K P m c (1) を受理すると（ステップ S312）、メモリカード 112 のメモリ 1412 中の暗号化コンテンツデータ [D c] K c を携帯電話機 102 に対して出力する（ステップ S314）。

【0119】

携帯電話機 102 から暗号化コンテンツデータ [D c] K c が携帯電話機 100 に対して送信され（ステップ S316）、携帯電話機 100 がこれを受信すると（S318）、転送された暗号化コンテンツデータ [D c] K c をメモリカード 110 は、メモリカード 110 のメモリ 1412 に格納する（ステップ S320）。

【0120】

続いて、メモリカード 112 においては、メモリカード 112 のメモリ 1412 内の暗号化されたライセンス情報データ [K c, L i c e n s e] K m c (2) を秘密復号キー K m c (2) により復号する（ステップ S322）。

【0121】

続いて、メモリカード 112 は、メモリカード 110 から送信されたメモリカード 110 の公開暗号化キー K P m c (1) によりコンテンツキーデータ K c およびライセンス情報データ L i c e n s e を暗号化して、データ [K c, L i c e n s e] K m c (1) を生成し（ステップ S324）、これを携帯電話機 102 に対して出力する（ステップ S326）。

【0122】

続いて図 9 を参照して、携帯電話機 102 から携帯電話機 100 へ、暗号化されたデータ [K c, L i c e n s e] K m c (1) が送信されると（ステップ S328）、携帯電話機 100 はこれを受信して（ステップ S330）、メモリカード 110 は、転送されたデータ [K c, L i c e n s e] K m c (1) を受理する（ステップ S332）。

【0123】

続いて、メモリカード110は、この受信したデータ [Kc, License] Kmc (1) をメモリカード110のメモリ1412に格納し (ステップS334)、続いて、秘密復号キーKmc (1) によって、このデータを復号して、抽出されたライセンス情報データLicenseをライセンス情報保持部1500に格納する (ステップS336)。

【0124】

メモリカード110において、ライセンス情報データLicenseのライセンス情報保持部1500への格納が完了すると、携帯電話機100から携帯電話機102へ配信受理が送信され (ステップS338)、携帯電話機102において、この配信受理が受信されると (ステップS340)、メモリカード112内のライセンス情報保持部1500のライセンス情報データLicenseの消去動作が行なわれる (ステップS342)。

【0125】

このメモリカード112内におけるライセンス情報データLicenseの消去が完了し (ステップS342)、かつ、メモリカード112のメモリ1412内のデータ消去を行なうか否かの確認をユーザ2が携帯電話機102のキータッチ部1108を介して行なうと (ステップS344)、続いて、メモリカード112のコントローラ1420はメモリ内のデータ消去を行なうか否かの判断を行ない (ステップS346)、ステップS344において、メモリ1412内のデータ消去が確認されている場合、メモリカード112のメモリ1412内のデータ [Dc] Kcおよび [Kc, License] Kmc (2) の消去動作を行ない (ステップS348)、処理が終了する (ステップS350)。

【0126】

一方、メモリ内のデータ消去が許可されない場合 (ステップS346)、そのまま処理が終了する (ステップS350)。

【0127】

メモリ内のデータ消去が許可されていない場合においても、メモリカード112内のライセンス情報保持部1500内のライセンス情報データLicense

が消去されているので、メモリカード112は、新たにコンテンツキーデータKcおよびライセンス情報データLicenseをサーバ30から配信してもらい、ライセンス情報保持部1500にライセンス情報を保持しない限り、暗号化コンテンツデータ[Dc]Kcの再生処理を行なうことはできない。

【0128】

[ユーザID、保守情報の変更処理]

図10は、本発明のメモリカード110の保守情報（メディア消去フラグ、追記フラグ、コンテンツ再生フラグ、コンテンツ消去フラグ）またはユーザIDデータUser-IDmの変更指示の処理を説明するためのフローチャートである。

【0129】

まず変更処理が開始されると、ユーザは、携帯電話機100のタッチキー部1108等から、保守情報またはユーザIDデータの変更指示を行なう（ステップS400）。

【0130】

続いて、メモリカードに、ユーザIDデータが登録されているか否かの判断が行なわれ（ステップS402）、ユーザIDデータが登録されている場合、メモリカード110のコントローラ1420は、携帯電話機100のユーザID保持部1107から携帯電話機100に登録されているユーザIDデータUser-IDhを入手する（ステップS404）。

【0131】

続いて、コントローラ1420は、携帯電話機100に登録されているユーザIDデータUser-IDhの値と、メモリカードのユーザID保持部1520に登録されているユーザIDデータUser-IDmとの比較を行ない（ステップS406）、一致している場合は、保守情報またはユーザIDの変更を行ない（ステップS408）、処理が終了する（ステップS412）。ここで、ユーザIDデータの変更とは、すでに登録されているユーザIDデータの値を別の値に書きかえることであってもかまわないし、また、すでに登録されているユーザIDデータの値を消去することであってもかまわない。また、ユーザIDを複数個

登録できる場合は、ユーザIDデータを追加する構成であっても良い。

【0132】

また、この場合、保守情報の変更は、第1の保守情報保持部1520中のメディア単位の管理データの変更でもかまわないし、第2の保守情報保持部1540中のコンテンツデータ単位の管理データ単位の変更でもかまわない。

【0133】

一方、ステップS402において、メモリカードにユーザIDが登録されていない場合、コントローラ1420は、携帯電話機に登録されたユーザID情報との比較を行なうことなく、保守情報またはユーザIDデータの変更処理を行ない（ステップS408）、処理が終了する（ステップS412）。

【0134】

一方、メモリカードにユーザIDが登録されている場合において、ステップS406において、携帯電話機のユーザIDとメモリカードのユーザIDとが一致しない場合は、コントローラ1420から携帯電話機100に対して変更不可の通知がされ（ステップS410）、処理が終了する（ステップS412）。

【0135】

携帯電話機100では、変更不可の通知を受けると、ディスプレイ1110等を介して、ユーザに対し変更処理が許可されないことを通知する。

【0136】

〔再生処理（保守情報の考慮のある場合）〕

図11は、保守情報の考慮のある場合について、本発明のメモリカードのコンテンツデータDc(i)の再生処理を指示した場合のメモリカード110の動作を説明するためのフローチャートであり、保守情報の考慮を行なわない場合の図7と対比される図である。

【0137】

処理が開始されると、ユーザは携帯電話機100のタッチキー部1108のキー操作等により、複数のコンテンツデータのうちの あるコンテンツデータDc(i)の再生指示を行なう（ステップS500）。

【0138】

自然数 i は、メモ리카ードに記録された複数の音楽データを区別するものである。

【0139】

メモ리카ード 110 のコントローラ 1420 は、この再生指示に応じて、ライセンス情報保持部 1500 中に保持されたコンテンツデータ $Dc(i)$ に対応するライセンス情報データ $License(i)$ の内容を確認する（ステップ S502）。たとえば、ライセンス情報データ $License(i)$ の値により、再生回数が制限されている場合、この制限範囲以内であるならば、再生可能と判断され、処理は次のステップに移行する。

【0140】

一方、ライセンス情報データ $License(i)$ により、再生不可が指定されている場合は、コントローラ 1420 は、携帯電話機 100 に対して再生不可の通知を出力し（ステップ S512）、処理が終了する（ステップ S520）。

【0141】

再生可能であると判断された場合、続いて、コントローラ 1420 は、コンテンツデータ $Dc(i)$ に対するコンテンツデータ単位の保守情報を第2の保守情報保持部 1540 に対して照会し、コンテンツ再生フラグの値を確認する（ステップ S504）。当該コンテンツデータ $Dc(i)$ に対する再生が可能である状態にコンテンツ再生フラグが設定されている場合、コントローラ 1420 に制御されて、復号処理部 1416 は、メモリ 1412 中に保持されている暗号化されたデータ $[Kc(i), License(i)] Kmc(1)$ を、秘密復号キー $Kmc(1)$ により復号する（ステップ S514）。

【0142】

このようにしてコンテンツキー $Kc(i)$ が、復号抽出され携帯電話機 100 の音楽再生部 1508 に対して出力される（ステップ S516）。

【0143】

さらに、メモリ 1412 からは暗号化されたコンテンツデータ $[Dc(i)] Kc(i)$ が、携帯電話機 100 の音楽再生部 1508 に対して出力され（ステップ S518）、処理が終了する（S520）。

【0144】

一方、ステップS504において、コンテンツ再生フラグのレベルにより、再生禁止が指示されている場合は、続いて、ユーザID保持部1520中にユーザIDが登録されているか否かの判断が行なわれる（ステップS506）、登録されていない場合、処理はステップS514に進み、コンテンツキーデータ $Kc(i)$ の復号抽出および暗号化されたコンテンツデータ $[Dc(i)]Kc(i)$ の出力が行なわれる。

【0145】

これに対して、ユーザID保持部1520中にユーザIDが登録されている場合、コントローラ1420は、携帯電話機100のユーザID保持部1107から携帯電話機100のユーザIDデータを取得し（ステップS508）、携帯電話機100に登録されたユーザIDデータ $User-IDh$ と、メモリカードに登録されているユーザIDデータ $User-IDm$ の値が一致しているか否かの判断を行なう（ステップS510）。

【0146】

携帯電話機100とメモリカード110のユーザIDが一致している場合は、処理はステップS514に移行し、コンテンツキーの抽出および暗号化されたコンテンツデータの出力が行なわれる。

【0147】

一方、携帯電話機100とメモリカード110のユーザIDが一致しない場合（ステップS510）、コントローラ1420は、携帯電話機100に対して再生不可の通知を行ない（ステップS512）、処理は終了する（ステップS520）。

【0148】

以上のような処理により、コンテンツデータごとに、ライセンス情報データに基づいた著作権保護ならびにユーザIDデータや保持情報に基づいたユーザ保護を行なった上で、コンテンツデータ（音楽データ）の再生処理を行なうことが可能となる。

【0149】

〔消去処理〕

図 1 2 は、メモ리카ード 1 1 0 中に保持されたコンテンツデータの消去動作を説明するためのフローチャートである。

【0 1 5 0】

処理が開始され、ユーザが携帯電話機 1 0 0 のキータッチ部 1 1 0 8 等からコンテンツデータ D c (i) の消去指示を行なう (ステップ S 6 0 0) 。まず、メモ리카ード 1 1 0 のコントローラ 1 4 2 0 は、メモ리카ード 1 1 0 に対する保守情報を記録した第 1 の保守情報保持部 1 5 2 0 中のメディア消去フラグの値を確認する (ステップ S 6 0 2) 。

【0 1 5 1】

メディア消去フラグにより、消去可能が指示されている場合処理は次のステップに進み、消去禁止が指示されている場合は、コントローラ 1 4 2 0 は、携帯電話機 1 0 0 に対して消去不可の通知を行ない (ステップ S 6 1 0) 、処理は終了する (ステップ S 6 1 2) 。

【0 1 5 2】

メディア消去フラグが消去可能を指定している場合、コントローラ 1 4 2 0 は、さらに、消去が指示されたコンテンツデータ D c (i) に対するコンテンツデータ単位の保守情報を第 2 の保守情報保持部 1 5 4 0 に対して照会し、コンテンツ消去フラグの値を確認する (ステップ S 6 0 4) 。

【0 1 5 3】

当該コンテンツデータ D c (i) の消去可能がコンテンツ消去フラグにより指定されている場合は、処理は次のステップに移行する。一方、消去禁止が指示されている場合は、コントローラ 1 4 2 0 は、消去不可の通知を携帯電話機 1 0 0 に対して出力し (ステップ S 6 1 0) 、処理は終了する (ステップ S 6 1 2) 。

【0 1 5 4】

コンテンツ消去フラグにより当該コンテンツデータ D c (i) の消去可能が指示されている場合は、続いて、コントローラ 1 4 2 0 は、ライセンス情報保持部 1 5 0 0 中のコンテンツデータ D c (i) に対応したライセンス情報データ L i c e n s e (i) の消去動作を行ない (ステップ S 6 0 6) 、メモリ 1 4 1 2 中

に保持された当該コンテンツデータに対応する暗号化されたコンテンツデータ [Dc(i)] Kc(i) およびこれに対応する暗号化されたコンテンツキーおよび暗号化されたライセンス情報データ [Kc(i), License(i)] Km c(1) の消去動作を行なって (ステップ S608)、処理が終了する (ステップ S612)。

【0155】

以上のような処理を行なうことで、メモリカードごとに消去動作が可能か否かの指定ができるとともに、各コンテンツデータ単位で消去動作が許可されるかどうかは保守情報により指定されているので、当該コンテンツデータを配信されたユーザの許可なく、メモリ 1412 中のコンテンツデータが消去されてしまうことを防止することが可能となる。

【0156】

[移動処理 (保守情報を考慮した場合：コンテンツデータの出力側)]

図 13 は、保守情報を考慮した場合において、メモリカード 112 を移動元としてコンテンツデータの移動処理を行なう場合の処理の流れを説明するためのフローチャートであり、図 8 および図 9 で説明したカード 112 の処理と対比される図である。

【0157】

処理が開始されると、まず、ユーザは、携帯電話機 102 のキータッチ部 1108 等を介して、コンテンツデータ Dc(i) の移動指示を行ない (ステップ S700)、続いて、メモリカード 112 のコントローラ 1420 は、まず第 1 の保守情報保持部 1520 に登録されたメディア単位の保守情報を照会して、メディア消去フラグの値を確認する (ステップ S702)。

【0158】

メディア消去フラグが消去可能を指示している場合は、処理は次のステップに移行し、消去禁止が指示されている場合は、メモリカード 112 のコントローラ 1420 は、携帯電話機 102 に対して移動不可の通知を行なって (ステップ S720)、処理は終了する (ステップ S722)。

【0159】

メディア消去フラグが消去可能を指示している場合は（ステップS702）、続いて、メモリカード112のコントローラ1420は、コンテンツデータDc(i)に対するコンテンツデータ単位の保守情報を第2の保守情報保持部1540に対して照会し、コンテンツ消去フラグのレベルを確認する（ステップS704）。

【0160】

当該コンテンツデータDc(i)に対する消去禁止が指示されている場合は、コントローラ1420は、携帯電話機102に対して移動不可を通知して（ステップS720）、処理は終了する（ステップS722）。

【0161】

一方、コンテンツ消去フラグが消去可能を指示している場合は、メモリカード112のコントローラ1420は、KPmc(1)保持部1405から、公開暗号化キーKPmc(1)を取得し（ステップS706）、続いて、メモリ1412中に格納されている暗号化されたコンテンツデータ[Dc(i)]Kc(i)を携帯電話機100を介して、移動先のメモリカード110に対して出力する（ステップS708）。

【0162】

続いて、メモリカード112のコントローラ1420は、復号処理部1416を制御して、メモリ1412中に保持されたデータ[Kc(i), License(i)]Kmc(2)を、自身の秘密復号鍵Kmc(2)により復号する（ステップS710）。

【0163】

さらに、メモリカード112のコントローラ1420は、暗号化処理部1414を制御して、この復号されたコンテンツキーデータおよびライセンス情報データを、移動先のメモリカード110から送信された移動先のメモリカード110に対する公開暗号化キーKPmc(1)により暗号化して、データ[Kc(i), License(i)]Kmc(1)を生成して、携帯電話機102を介して、移動先のメモリカード110に対して出力する（ステップS712）。

【0164】

続いて、メモ리카ード112のコントローラ1420は、ライセンス情報保持部1500中に保持されたコンテンツデータDc(i)に対応したライセンス情報データLicense(i)の消去を行なう(ステップS714)。

【0165】

続いて、メモ리카ード112のコントローラ1420は、携帯電話機102のディスプレイ等を介して、ユーザにメモリ1412中のデータ消去を行なうか否かの確認を行ない、ユーザからキータッチ部1108等を介して消去が指示された場合は(ステップS716)、メモリ1412中の暗号化されたコンテンツデータ[Dc(i)]Kc(i)および暗号化されたコンテンツキーおよびライセンス情報データを消去して(ステップS718)、処理が終了する(ステップS722)。

【0166】

一方、ユーザがメモリ1412中のデータ消去を指示しなかった場合は、メモリ1412中の暗号化されたコンテンツデータ、暗号化されたコンテンツキーデータおよびライセンス情報データを消去することなく処理が終了する(ステップS722)。

【0167】

コンテンツデータの一括した移動の場合と同様に、メモリ1412内の暗号化されたコンテンツデータの消去を行なわなかった場合も、ライセンス情報保持部1500中の当該コンテンツデータDc(i)に対応したライセンス情報データは消去されているので、このままではメモ리카ード110は当該コンテンツデータの再生処理を行なうことはできない。

【0168】

以上のようにして、コンテンツデータ単位で保守情報を参照しつつ、移動元のメモ리카ード112から移動先のメモ리카ード110に対してコンテンツデータの移動を行なうことが可能となる。

【0169】

[配信・移動処理(保守情報を考慮した場合:コンテンツデータの受け側)]

図14は、メモ리카ード110に対して、たとえば、移動動作において受信側

となっている場合、保守情報を考慮したときのコンテンツデータの追記を行なう処理を説明するためのフローチャートであり、図8および図9で説明したカード110の処理と対比される図である。

【0170】

コンテンツデータの追記としては、上述のとおり、コンテンツデータをメモリカード間で移動させる場合に受信してもよいし、あるいは、たとえば、携帯電話網を介して配信サーバ10から配信を受ける構成としてもよいし、街頭に設置されたコンテンツデータ販売機を介して、メモリカードに直接コンテンツデータが書込まれる構成としてもよい。

【0171】

処理が開始されると、ユーザ2は、携帯電話機102のキータッチ部1108等を介して、コンテンツデータDc(i)の移動(記録)指示をメモリカード110に対して与える(ステップS800)。

【0172】

続いて、メモリカード110のコントローラ1420は、メディア単位の保守情報を第1の保守情報保持部1520に対して照会し、追記フラグのレベルを確認する(ステップS802)。追記が禁止されている場合、コントローラ1420は、携帯電話機100に対して移動不可の通知を出力し(ステップS816)、処理が終了する(ステップS818)。この移動不可の通知は、携帯電話機100から携帯電話機102にさらに伝達される。

【0173】

一方、追記フラグにより追記可能が指示されている場合は、メモリカード110は、K P m c (1) 保持部1405から、メモリカード110に対する公開暗号化キーK P m c (1) を追記に対する移動元(メモリカード112)に対して出力し(ステップS804)、移動元から暗号化されたコンテンツデータ[Dc(i)] Kc(i)を受けて、メモリ1412に格納する(ステップS806)。

【0174】

続いて、メモリカード110は、携帯電話機100を介して、移動元からメモ

リカード110に対する公開暗号化キーK P m c (1)により暗号化されたコンテンツキーデータおよびライセンス情報データ[K c (i)、L i c e n s e (i)] K m c (1)を受け、メモリ1412に対して格納する(ステップS810)。

【0175】

続いて、コントローラ1420により制御されて、復号処理部1416がメモリ1412中に保持されたコンテンツキーデータおよびライセンス情報データを秘密復号キーK m c (1)により復号し(ステップS812)、復号されたライセンス情報データL i c e n s e (i)をライセンス情報保持部1500に格納して(ステップS814)、処理が終了する(ステップS818)。

【0176】

以上のような処理を行なうことで、コンテンツデータ単位の追記動作を行なうことが可能となる。

【0177】

すなわち、第1には、メモリカードにはユーザIDデータU s e r - I D mが保持され、携帯電話機には、ユーザIDデータU s e r - I D hが保持される構成とすることで、メモリカードのユーザと携帯電話機のユーザとが一致しないかぎり、保守情報やユーザIDデータU s e r - I D mを変更することが出来ないため、正規にコンテンツデータを購入したユーザを保護することが可能となる。

【0178】

しかも、第2には、再生処理、移動処理、消去処理等において、ユーザの設定した保守情報により、コンテンツデータが正規の購入者に無断で、再生されたり、消去されたり、他のメモリカードに移動されたりすることを防止することが可能となる。

【0179】

〔実施の形態2〕

実施の形態1のメモリカードでは、メモリカードのユーザと携帯電話機のユーザとが一致しないかぎり、保守情報やユーザIDデータU s e r - I D mを変更することが出来ない構成とし、しかも、再生処理、移動処理、消去処理等におい

て、ユーザの設定した保守情報により、コンテンツデータが正規の購入者に無断で、再生されたり、消去されたり、他のメモリカードに移動されたりすることを防止する構成であった。

【0180】

実施の形態2のメモリカードでは、さらに、コンテンツデータの移動の制限として、メモリカードのユーザIDデータとそれが装着される携帯電話機のユーザIDデータの2つのユーザIDが一致しない場合には、コンテンツデータに対応したライセンス情報の移動または消去が禁止される。

【0181】

まず、実施の形態1と同様に、ユーザIDデータUser-IDmをメモリカード110のユーザID保持部1520が記録し、携帯電話機100においてもユーザID保持部1107にユーザIDデータUser-IDhを記録しているものとする。

【0182】

図15は、このような構成を有する携帯電話機100が、メモリカード110を装着した状態で、配信サーバ10および配信キャリア（携帯電話会社）20を介して、コンテンツデータの配信を受ける状態を示す概念図である。

【0183】

図15に示した構成では、i番目のコンテンツデータDc(i)に対する再生情報Read(i)として、コンテンツ復号キーKc(i)、ライセンスIDデータLicense-ID(i)およびコンテンツデータの配信を受けた際のユーザを示すユーザIDデータUser-ID(i)の組合せを用いた場合の構成を示す。

【0184】

ここで、このコンテンツデータごとに対応し、ライセンス情報中に含まれるユーザIDデータUser-ID(i)は、当該コンテンツデータ配信の際にユーザIDデータUser-IDhの値が転写される。

【0185】

配信サーバ10から携帯電話網を介して暗号化されたコンテンツデータDc(

i) が配信された場合、携帯電話機に記録されているユーザIDデータUser-IDhは“09000000001”であり、かつ、メモリカード110中に保持されるユーザIDデータUser-IDmも“09000000001”という値が保持されているものとする。このとき、コンテンツデータDc(i)に対応した再生情報Read(i)中のユーザIDデータUser-ID(i)も“09000000001”であるものとする。

【0186】

再生情報Read(i)は、暗号化キーKPmc(1)により暗号化されたデータ[Read(i)]Kmc(1)として、メモリカード110中のメモリ1412に保持されているものとする。

【0187】

さらに、メモリカード110のメモリ1412中には暗号化されたコンテンツデータ[Dc(i)]Kc(i)が保持されている。

【0188】

図16は、2つのメモリカード110と112との間で、再生情報の移動が許可される場合を示す概念図である。

【0189】

図16に示した場合は、送信元の携帯電話機100では、メモリカード110のユーザIDデータUser-IDmと、携帯電話機100のユーザIDデータUser-IDhとが一致している。

【0190】

このような場合には、メモリカード110からメモリカード112に対して、暗号化コンテンツデータのみならず暗号化再生情報Read(i)の移動が許可されて、暗号化されたコンテンツデータ[Dc(i)]Kc(i)を携帯電話機102の側でも再生することが可能になる。メモリカード110のライセンス情報保持部1500からは、実施の形態1と同様に、暗号化コンテンツデータと再生情報の双方がメモリカード112に移動するのに伴って、再生情報が消去される。

【0191】

図 17 は、2 つのメモリカード 110 と 112 との間で、再生情報の移動が許可されない場合を示す概念図である。

【0192】

送信元の携帯電話機 100 では、メモリカード 110 のユーザ ID データ $User-ID_m$ と、携帯電話機 100 のユーザ ID データ $User-ID_h$ とは一致していない。

【0193】

したがって、このような場合は、メモリカード 110 のコントローラ 1420 は、メモリカード 110 のメモリ 1412 中の再生情報 $Read(i)$ のメモリカード 112 への転送を許可しない。

【0194】

このような構成とすることで、正規のユーザ以外が、無断でコンテンツデータを他のメモリカードに移動することを禁じることが可能となる。

【0195】

再生情報としてはコンテンツキー（暗号化コンテンツデータの復号キー）のみを含む構成としてもよいし、コンテンツキーとライセンス情報データとの組合せとしてもよい。

【0196】

ただし、再生情報をコンテンツキーとユーザ ID データとした場合、または、コンテンツ復号キー、ライセンス情報データおよびユーザ ID データの組合せとした場合は、以下のような処理を行なうことが可能である。

【0197】

すなわち、以上の説明では、携帯電話機のユーザ ID データとメモリカードのユーザ ID データとの一致／不一致に応じて、コンテンツデータに対応したライセンス情報の移動または消去が禁止される構成であった。

【0198】

上述のとおり、再生情報 $Read(i)$ として、言いかえると、コンテンツデータごとに、ユーザ ID データ $User-ID(i)$ がライセンス情報保持部 1500 およびメモリ 1412 に格納されている場合は、このユーザ ID データ U

ser-ID (i) の値と、メモリカードのユーザIDデータ User-IDm の値、携帯電話機のユーザIDデータ User-IDh の値とに応じて、再生情報の移動を許可するか否かを、コンテンツデータごとに判断して、処理することが可能である。

【0199】

すなわち、メモリカードに記録された再生情報に含まれるユーザIDデータ User-ID (i) と、メモリカードのユーザIDデータ User-IDm と携帯電話機に記憶されたユーザIDデータ User-IDh との関係から、コンテンツデータのライセンス情報の移動または消去が禁止されるという制御を行なうことが可能である。

【0200】

図18は、このようにコンテンツデータ単位で、再生情報の転送を制御する場合の構成を示す概念図である。

【0201】

なお、実施の形態1の図10で説明したのと同様に、携帯電話機のユーザIDデータ User-IDh とメモリカードのユーザIDデータ User-IDm と、コンテンツデータ Dc (i) に対応したユーザ情報データ中のユーザIDデータ User-ID (i) とが一致している場合にユーザIDデータ User-ID (i) を書きかえることで、ユーザIDに対する制限を解除することが可能である。また、コンテンツデータ Dc (i) に対応したユーザ情報データ中のユーザIDデータ User-ID (i) が記憶されていない場合は、ユーザIDに対する制限は、働かないものとする。

【0202】

以上のような構成とした場合、メモリカード110からメモリカード112へ再生情報の移動が行なわれた後の状態としては、たとえば、以下の5通りのような場合がある。

【0203】

まず、図18においても、図15と同様に、i 番目のコンテンツデータ Dc (i) に対する再生情報 Read (i) として、コンテンツ復号キー Kc (i) 、

ライセンスIDデータLicense-ID(i)およびコンテンツデータの配信を受けた際のユーザを示すユーザIDデータUser-ID(i)の組合せを用いる。

【0204】

また、携帯電話機100に記録されているユーザIDデータUser-IDhは“09000000001”であり、かつ、メモリカード110中に保持されるユーザIDデータUser-IDmも“09000000001”という値が保持されているものとする。携帯電話機102に記録されているユーザIDデータUser-IDhは“09000000002”であり、かつ、メモリカード112中に保持されるユーザIDデータUser-IDmも“09000000002”という値が保持されているものとする。

【0205】

さらに、再生情報Read(i)は、暗号化キーKPmc(1)により暗号化されたデータ[Read(i)]Kmc(1)として、メモリカード110中のメモリ1412に保持されているものとする。

【0206】

図18を参照して、まず、第1の場合としては、メモリカード110において、コンテンツデータDc(i)に対応した再生情報Read(i)中のユーザIDデータUser-ID(i)も“09000000001”であるものとする。この場合、メモリカード110のユーザIDデータUser-IDmと携帯電話機100のユーザIDデータUser-IDhが一致し、かつ、コンテンツデータKc(i)に対応したユーザIDデータUser-ID(i)もこれらと一致するので、再生情報の移動が許可され、かつ、メモリカード112に移動後も、再生情報Read(j)中のユーザIDデータUser-ID(j)は“09000000001”のままである。

【0207】

第2の場合としては、上記第1の場合の移動後に、携帯電話機102において、再生情報Read(j)中のユーザIDデータUser-ID(j)を“09000000002”にした場合である。

【0208】

第3の場合としては、上記第1の場合の移動後に、携帯電話機102において、再生情報Read(j)中のユーザIDデータUser-ID(j)を消去した場合である。

【0209】

第4の場合としては、もともと、再生情報Read(i)中のユーザIDデータUser-ID(i)は記録されていない場合である。この場合は、再生情報の移動が許可され、ユーザIDデータUser-ID(i)による移動の制限はない。

【0210】

第5の場合は、第4の場合において、さらにユーザが携帯電話機102の側で、再生情報Read(j)中のユーザIDデータUser-ID(j)を“0900000002”とした場合である。

【0211】

以上、第1から第5のいずれの場合も、メモ리카ード110のライセンス情報保持部1500からは、暗号化コンテンツデータと再生情報の双方がメモ리카ード112に移動するのに伴って、再生情報が消去される。

【0212】

図19は、これらに対して、このようにコンテンツデータ単位で、再生情報の転送を制御した場合に、ライセンス情報の移動が禁止されるときを示す概念図である。

【0213】

移動元の携帯電話機100においては、メモ리카ード110のユーザIDデータUser-IDmと、携帯電話機100のユーザIDデータUser-IDhとは一致しているものの、携帯電話機100のユーザIDデータUser-IDhと再生情報Read(i)中のユーザIDデータUser-ID(i)とが一致しないため、再生情報の移動が禁止される。

【0214】

このような構成により、メモ리카ードという携帯電話機から着脱可能な記録媒

動、複製においてはコンテンツデータとともに処理され、再生時には分離されて音楽データとは個別にアクセス可能となるように、暗号化コンテンツデータと同じメモリ 1 4 1 2 に記録される。

【0 2 2 0】

なお、以上の説明では、メモリカードとしての構成を説明したが、本発明はこのような構成に限定されることなく、より一般に、配信された暗号化コンテンツデータを再生出力する再生装置、たとえば、携帯電話機に対して着脱可能であって、かつ、暗号化コンテンツデータの配信のために必要なキーデータ等の授受を行う機能を有して、この暗号化コンテンツデータを受けて記録する装置に対して適用可能なものである。

【0 2 2 1】

さらに、本発明において、ユーザが音楽データなどのコンテンツデータを入手する経路としては、上述のとおり、携帯電話網や他の情報通信網を介したデータ配信に限られるものではなく、たとえば、多数のコンテンツデータを蓄えて街頭に設置されたコンテンツデータ販売機などにより販売される情報を記録する記録装置にも適用可能なものである。

【0 2 2 2】

今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は上記した説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【0 2 2 3】

【発明の効果】

以上説明したとおり、本願発明にかかる配信システムでは、正規のユーザが受信してメモリ中に格納したコンテンツデータに対して、正規ユーザのみが再生、消去、移動処理を行なうことが可能な構成となっているので、正当なユーザが、無断で行なわれる不当な処理により不利益を被るのを防止することが可能となる。

【図面の簡単な説明】

【図 1】 情報の配信を受けるための端末である携帯電話機 1 0 0 の構成を説明するための概略ブロック図である。

【図 2】 図 1 に示したメモ리카ード 1 1 0 の構成を説明するための概略ブロック図である。

【図 3】 本発明の記録媒体が用いられる情報配信システムの全体構成を概略的に説明するための概念図である。

【図 4】 図 3 に示した情報配信システムにおいて使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

【図 5】 図 3 に示した音楽サーバ 3 0 の構成を示す概略ブロック図である。

【図 6】 実施の形態 1 の情報配信システムにおけるコンテンツデータの配信動作を説明するためのフローチャートである。

【図 7】 メモ리카ード 1 1 0 に保持された暗号化コンテンツデータから、音楽情報を再生処理を説明するためのフローチャートである。

【図 8】 2 つのメモ리카ード間において、コンテンツデータおよびキーデータとの移動を行なう処理を説明するための第 1 のフローチャートである。

【図 9】 2 つのメモ리카ード間において、コンテンツデータおよびキーデータとの移動を行なう処理を説明するための第 2 のフローチャートである。

【図 1 0】 本発明のメモ리카ード 1 1 0 の保守情報またはユーザ ID データ User-IDm の変更指示の処理を説明するためのフローチャートである。

【図 1 1】 保守情報の考慮のある場合について、メモ리카ード 1 1 0 のコンテンツデータ Dc (i) の再生動作を説明するためのフローチャートである。

【図 1 2】 メモ리카ード 1 1 0 中に保持されたコンテンツデータの消去動作を説明するためのフローチャートである。

【図 1 3】 保守情報を考慮した場合において、移動処理を行なう場合の処理の流れを説明するためのフローチャートである。

【図 1 4】 移動動作において受信側となっている場合、保守情報を考慮したときの追記処理を説明するためのフローチャートである。

【図 1 5】 メモ리카ード 1 1 0 がコンテンツデータの配信を受ける状態を

示す概念図である。

【図16】 2つのメモ리카ード110と112との間で、再生情報の移動が許可される場合を示す概念図である。

【図17】 2つのメモ리카ード110と112との間で、再生情報の移動が許可されない場合を示す概念図である。

【図18】 コンテンツデータ単位で、再生情報の転送を制御する場合の構成を示す概念図である。

【図19】 コンテンツデータ単位で、再生情報の転送を制御した場合に、ライセンス情報の移動が禁止されるときを示す概念図である。

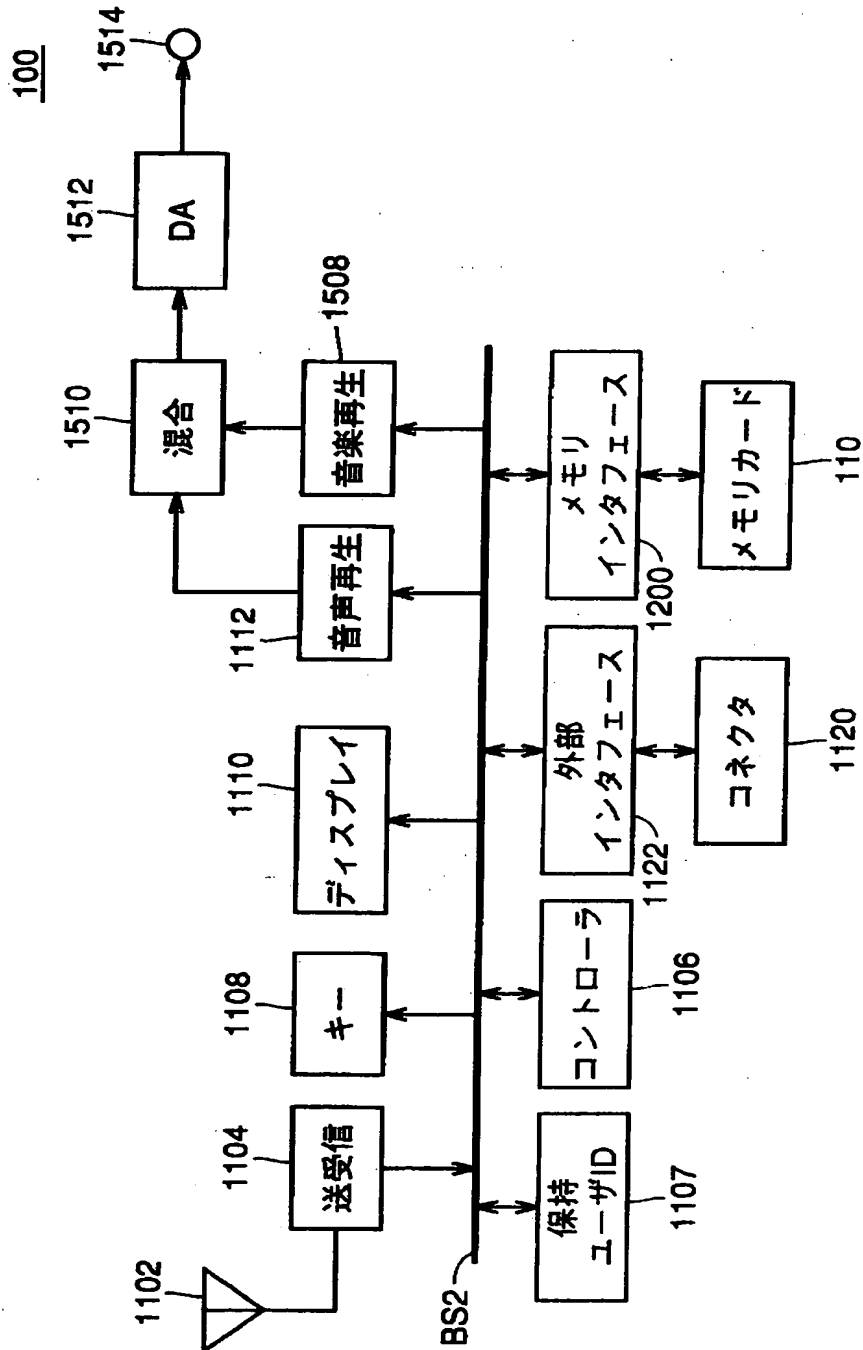
【符号の説明】

10 配信サーバ、20 配信キャリア、30 音楽サーバ、100, 101, 102, 103 携帯電話機、110, 112, 120, 122 メモ리카ード、130, 132 ヘッドホン、1102 アンテナ、1104 送受信機、1106 コントローラ、1107 ユーザID保持部、1108 タッチキー部、1110 ディスプレイ、1112 音声再生部、1200 メモリインタフェース、1404 復号処理部、1406 暗号化処理部、1408, 1409 切替スイッチ、1410 復号処理部、1412 メモリ、1414 暗号化処理部、1416 復号処理部、1420 コントローラ、1430 暗号化処理部、1432 セッションキー発生部、1434, 1435 切替スイッチ、1500 ライセンス情報保持部、1502 セッションキー発生部、1504 暗号化処理部、1506 復号処理部、1508 音楽再生部、1510 混合部、1512 デジタルアナログ変換器、1520 第1の保守情報保持部、1530 ユーザID保持部、1540 第2の保守情報保持部。

【書類名】

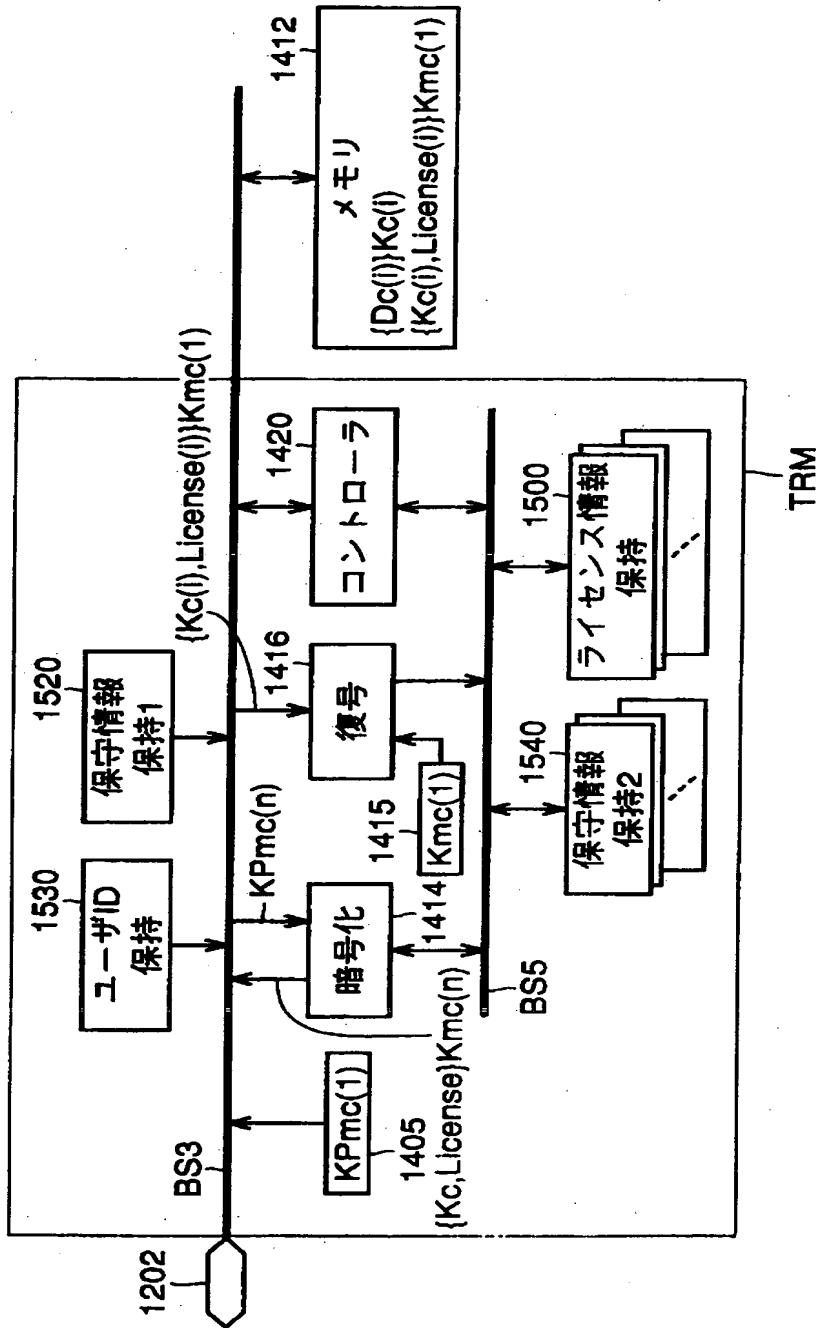
図面

【図 1】

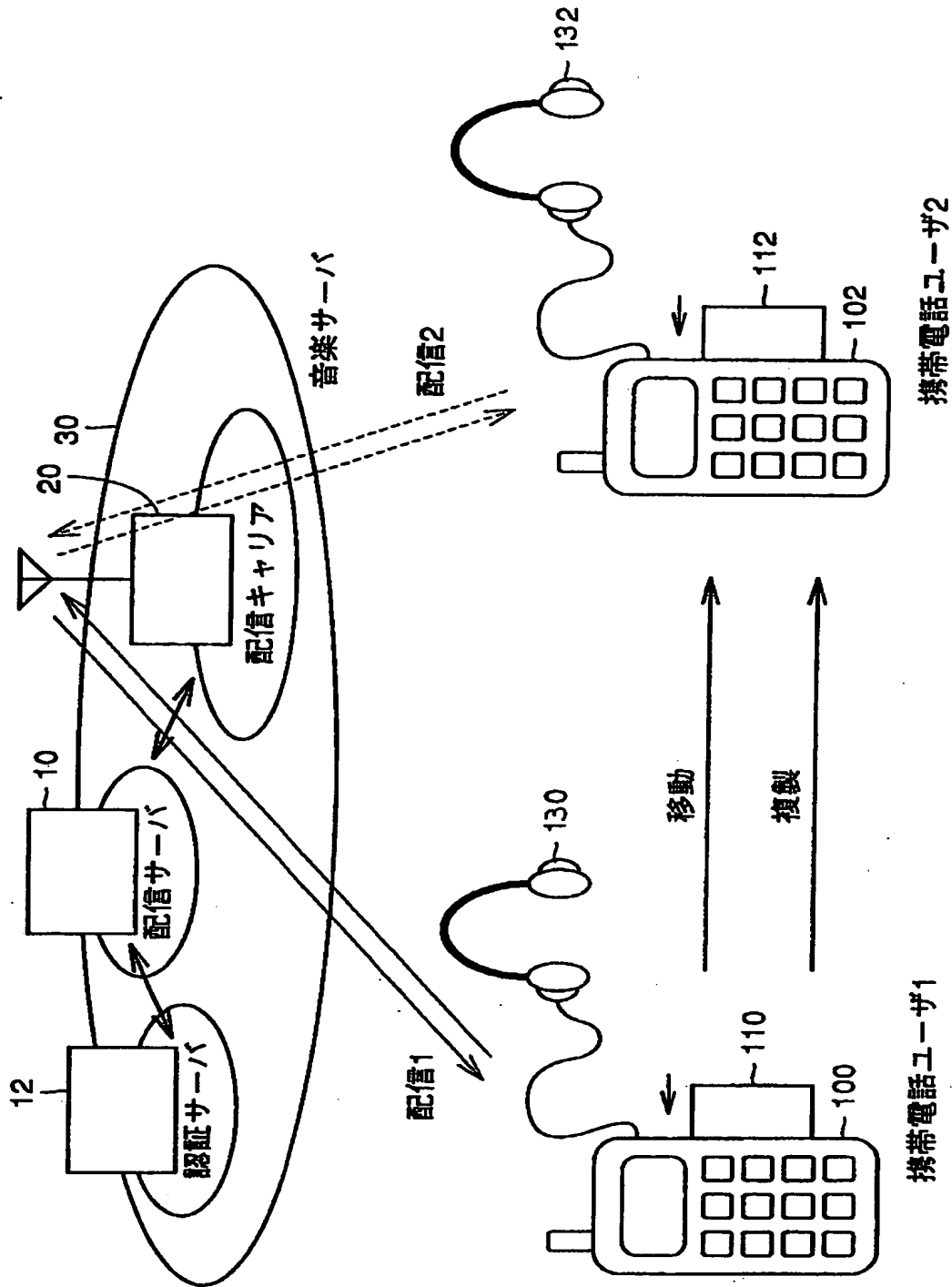


【図 2】

110



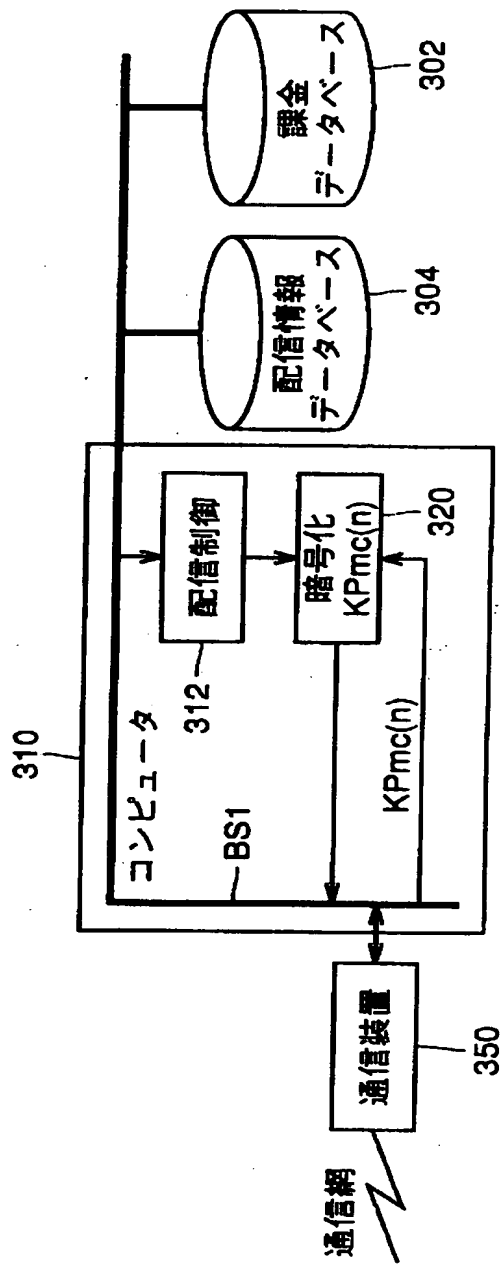
【図 3】



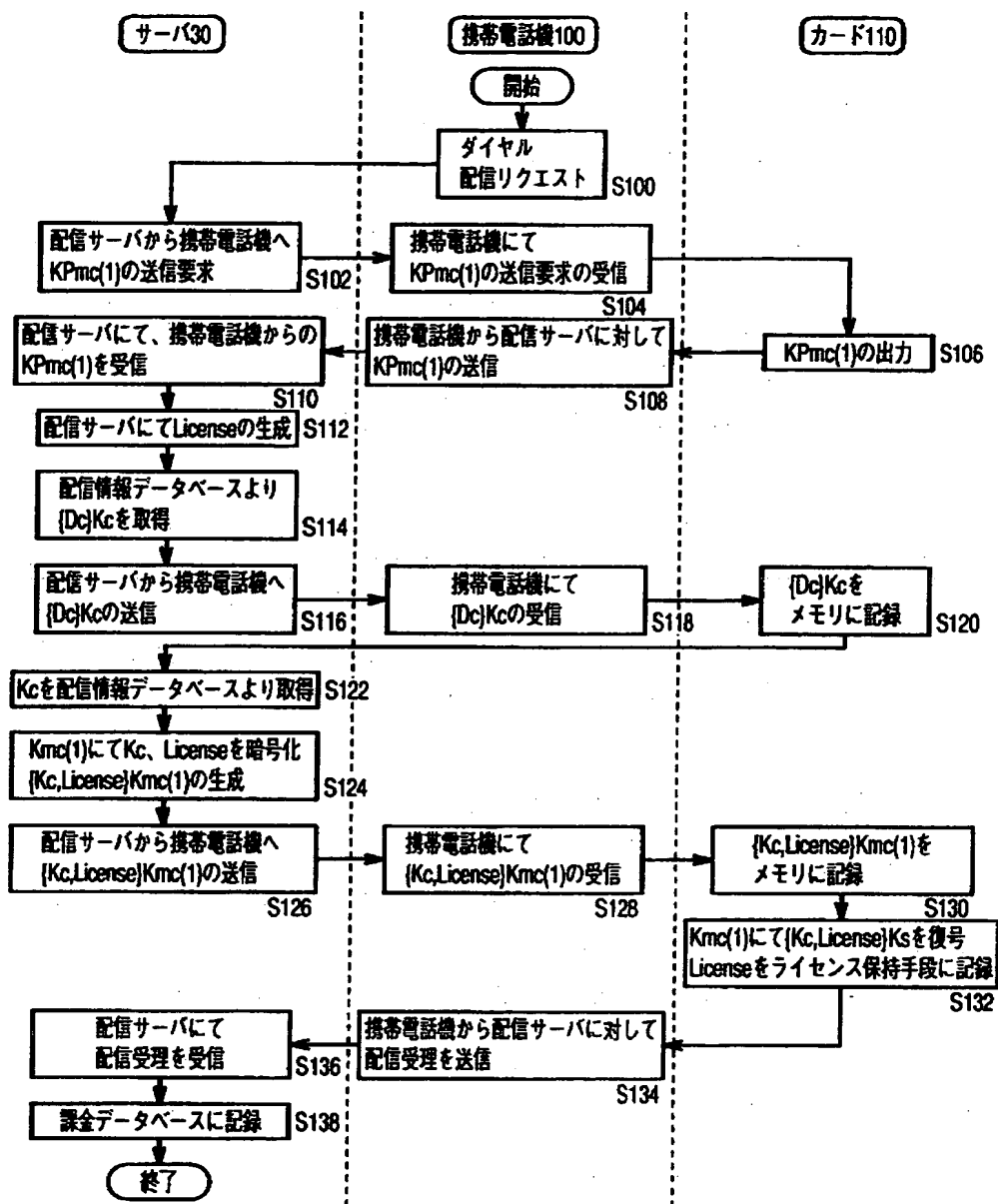
【図 4】

	記号	属性	特性	
メモリカード内 管理の鍵	Kmc(n)	秘密復号鍵		メモリカード毎に異なる
	KPmc(n)	公開暗号化鍵		Kmc(n)と対を成す。 KPmc(n)により暗号化されたデータ は、Kmc(n)で復号可能
	User-IDm	メモリカードのユーザ を識別する情報		例：ユーザの設定
メモリカード外 管理の鍵	User-IDh	携帯電話機ユーザを 識別する情報		例：電話番号
配信データ	Kc(l)	共通鍵	ライセン ス キー	暗号化コンテンツデータの復号鍵
	License(l)	再生に関する情報	コンテ ンツ データごと	例：曲目の特定情報 再生回数の制限情報
	Dc(l)	コンテンツデータ		例：音楽情報データ
	[Dc]Kc	暗号化コンテンツ データ		共通鍵Kcにより暗号化されたコンテ ンツデータ

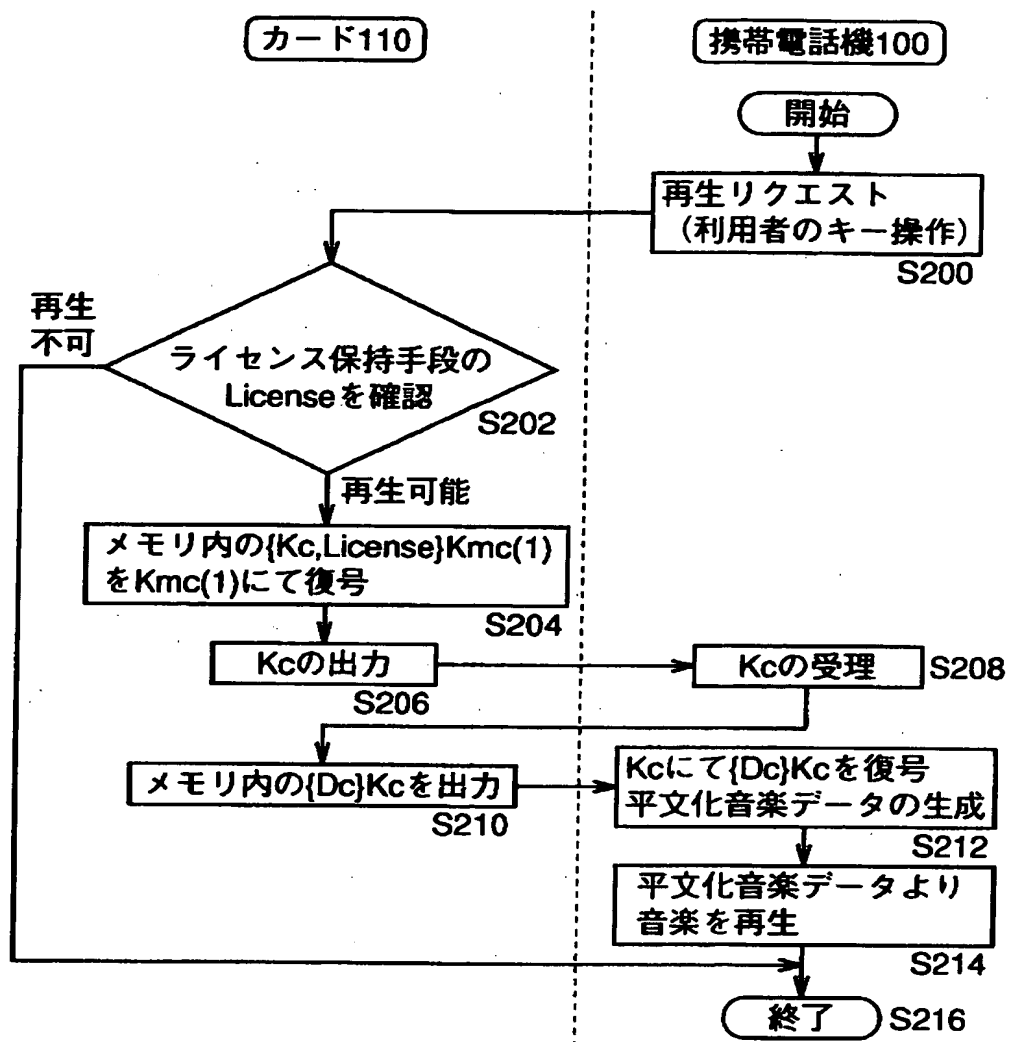
【図 5】



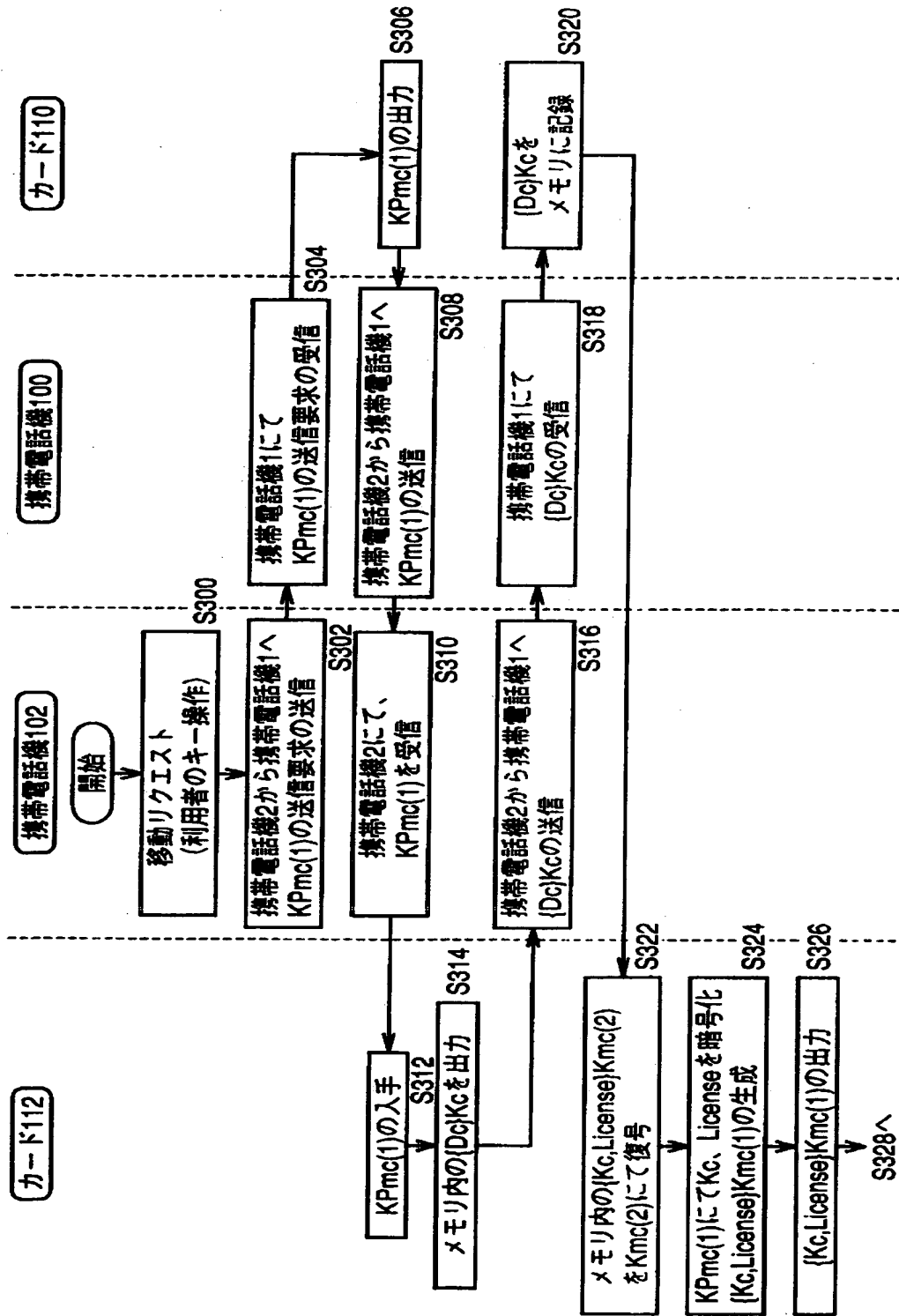
【図 6】



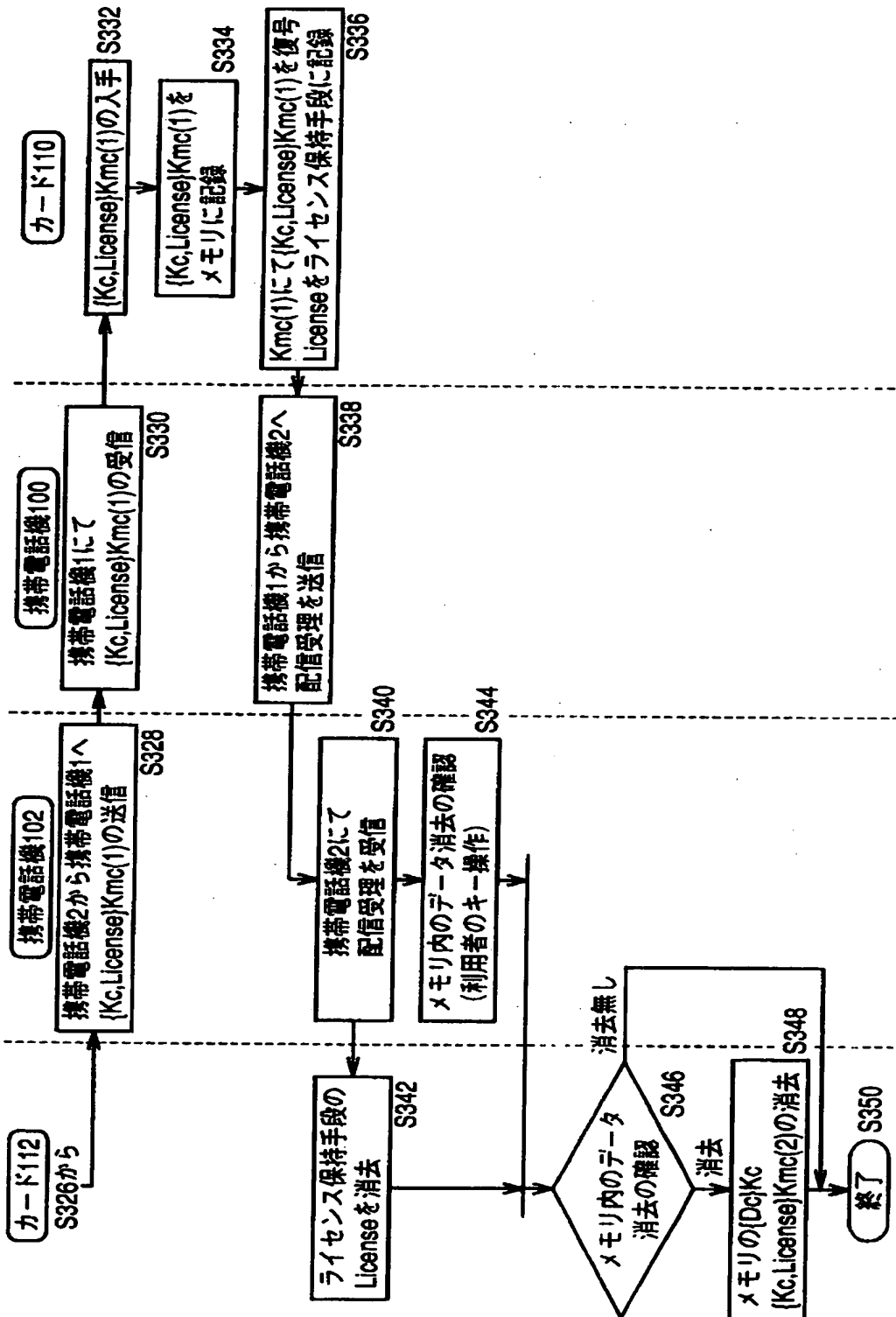
【図 7】



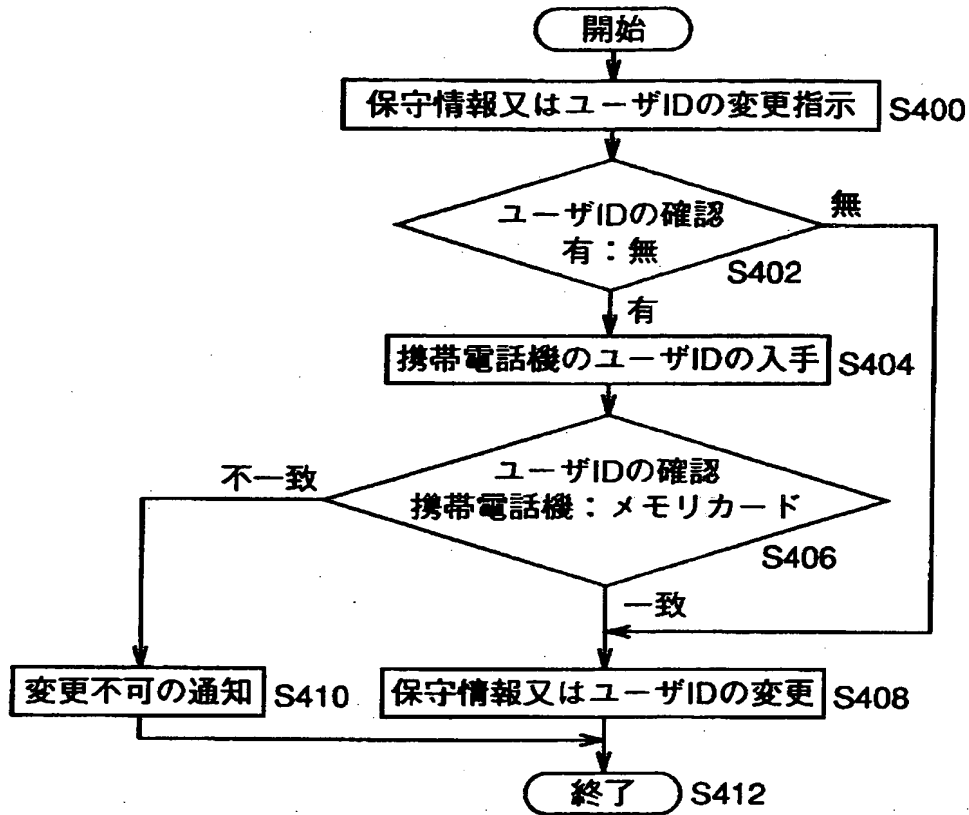
【図 8】



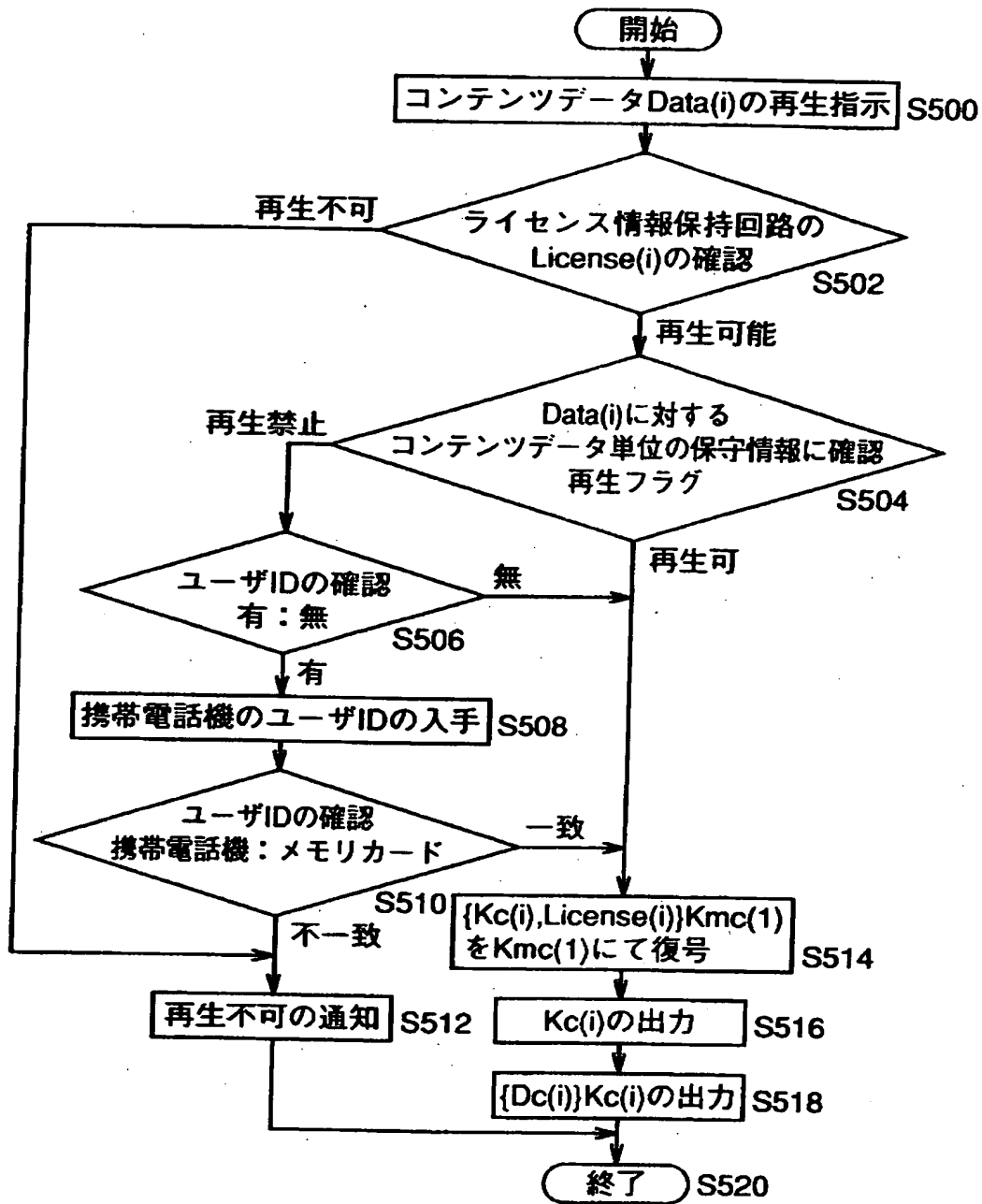
【図 9】



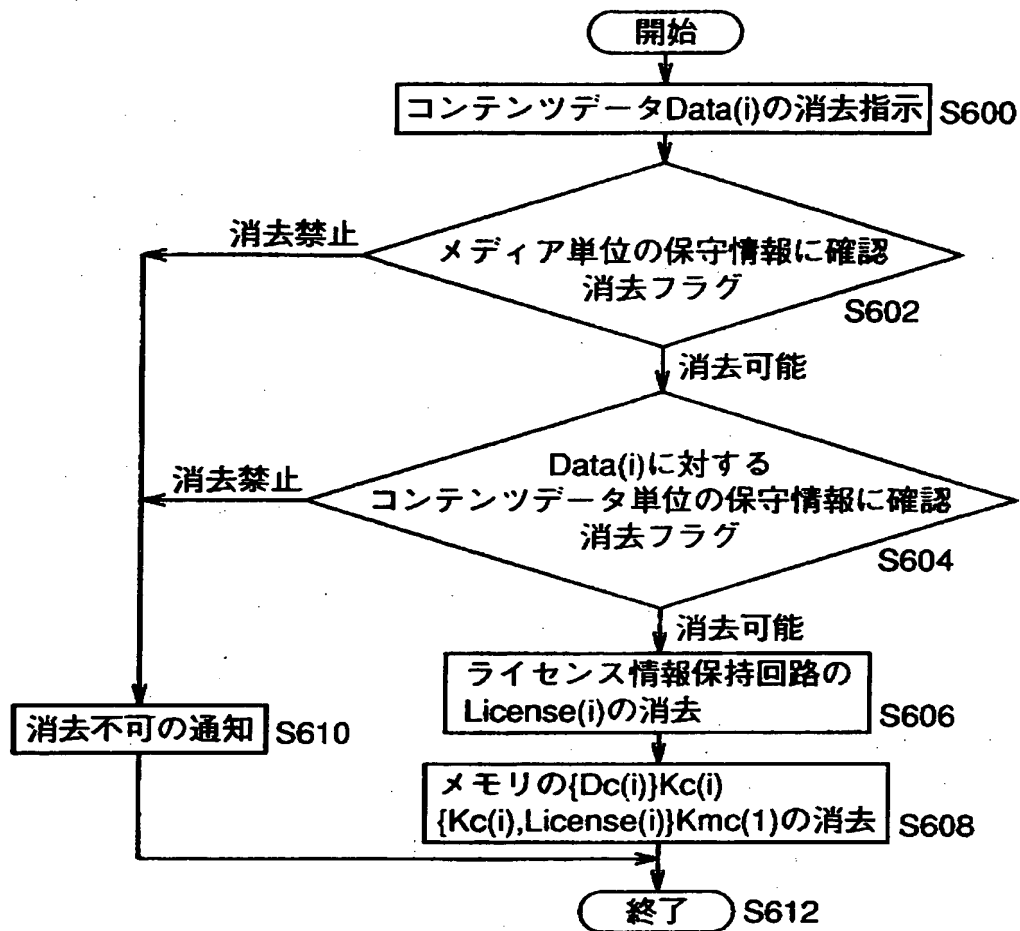
【図 10】



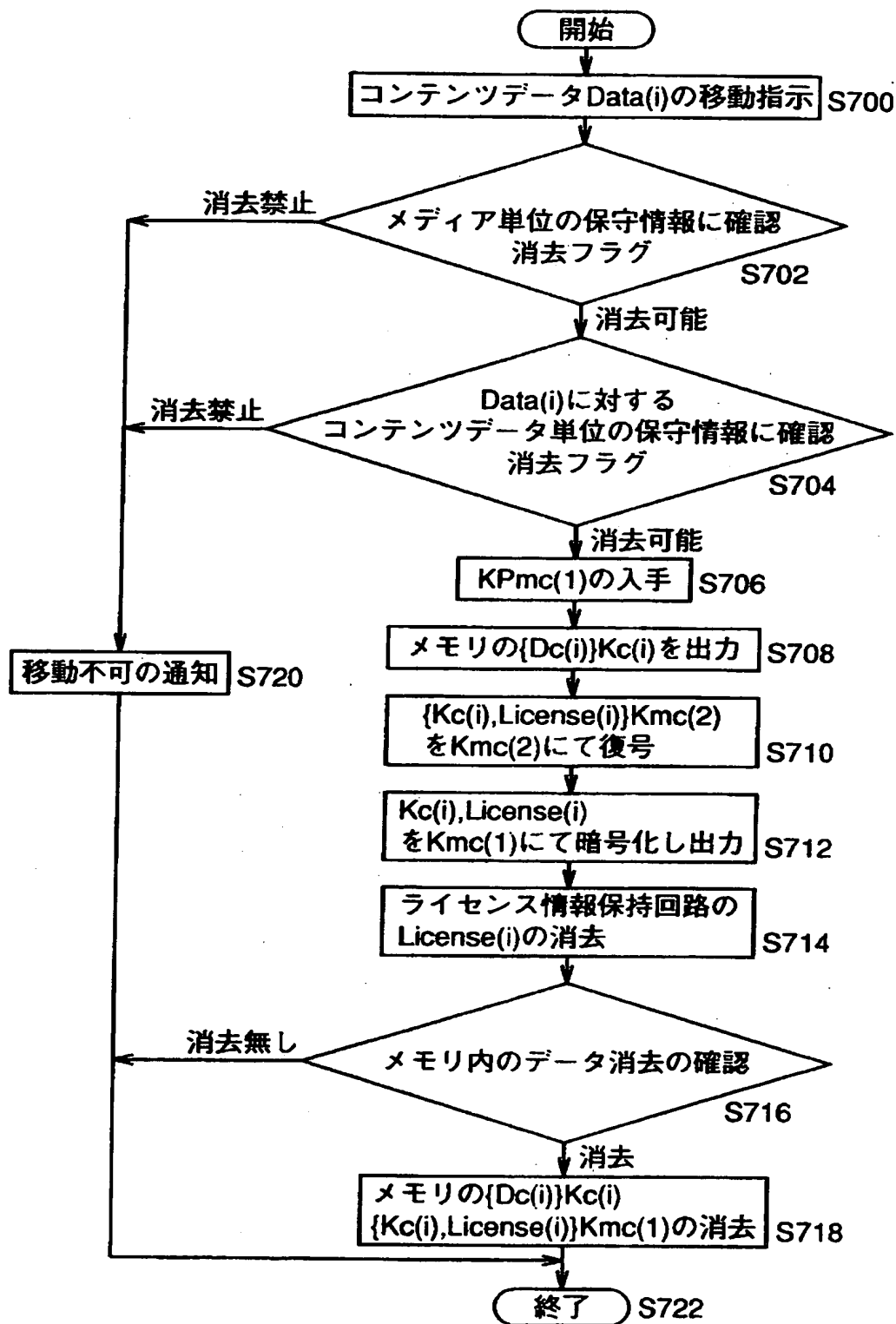
【図 1 1】



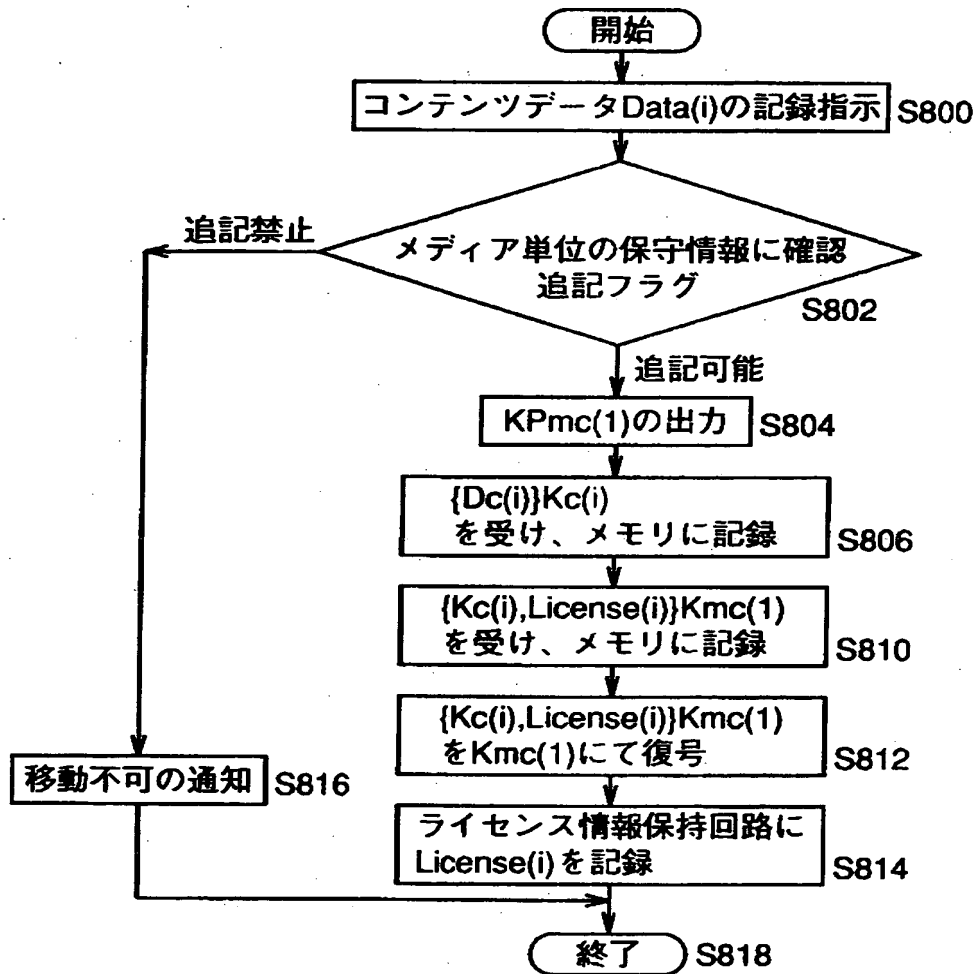
【図 1 2】



【図 13】

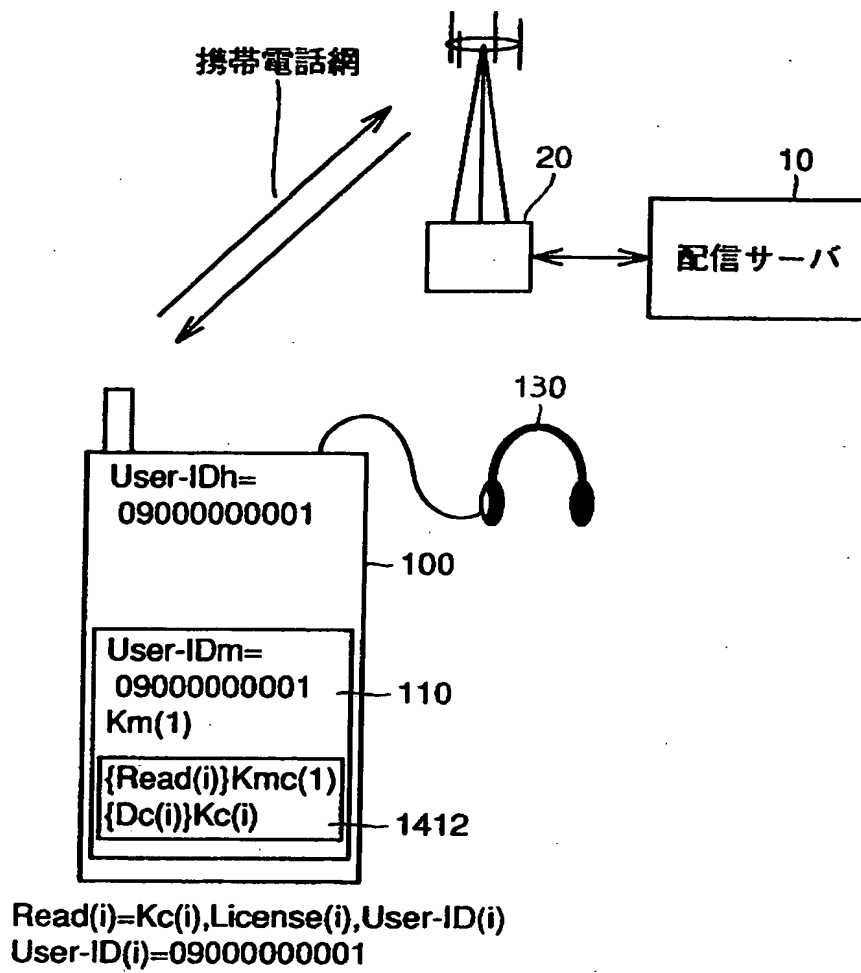


【図 1 4】



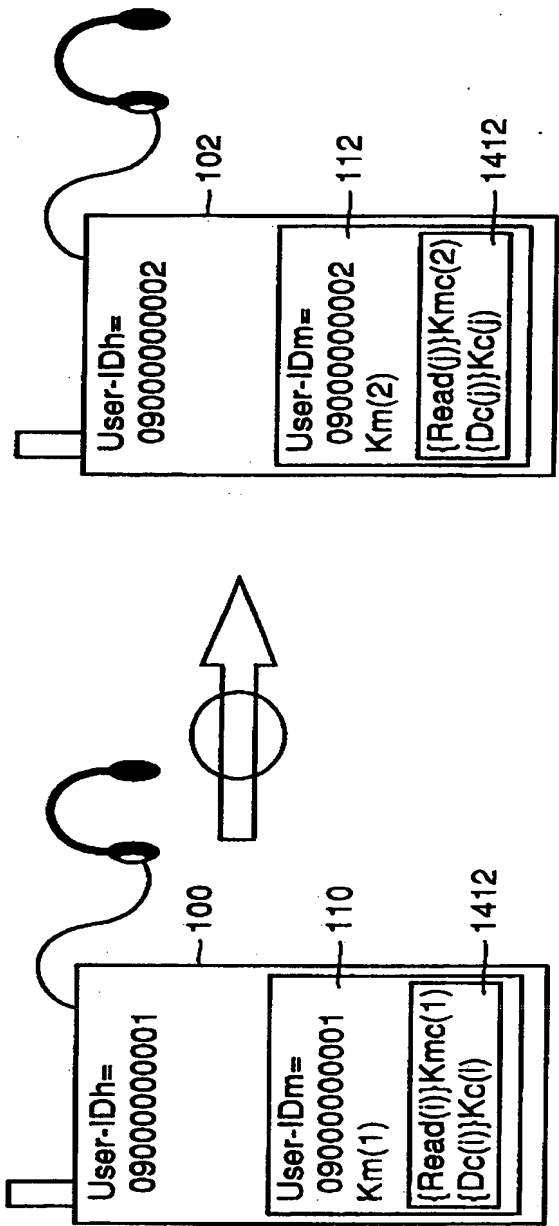
【図 1 5】

配信



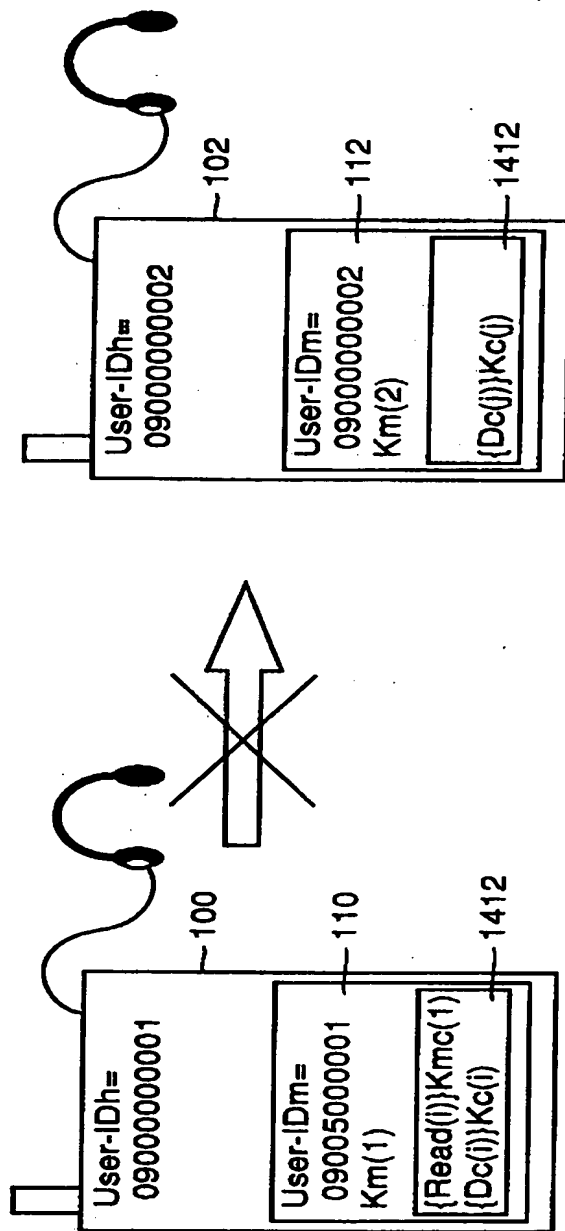
【図 1 6】

移動

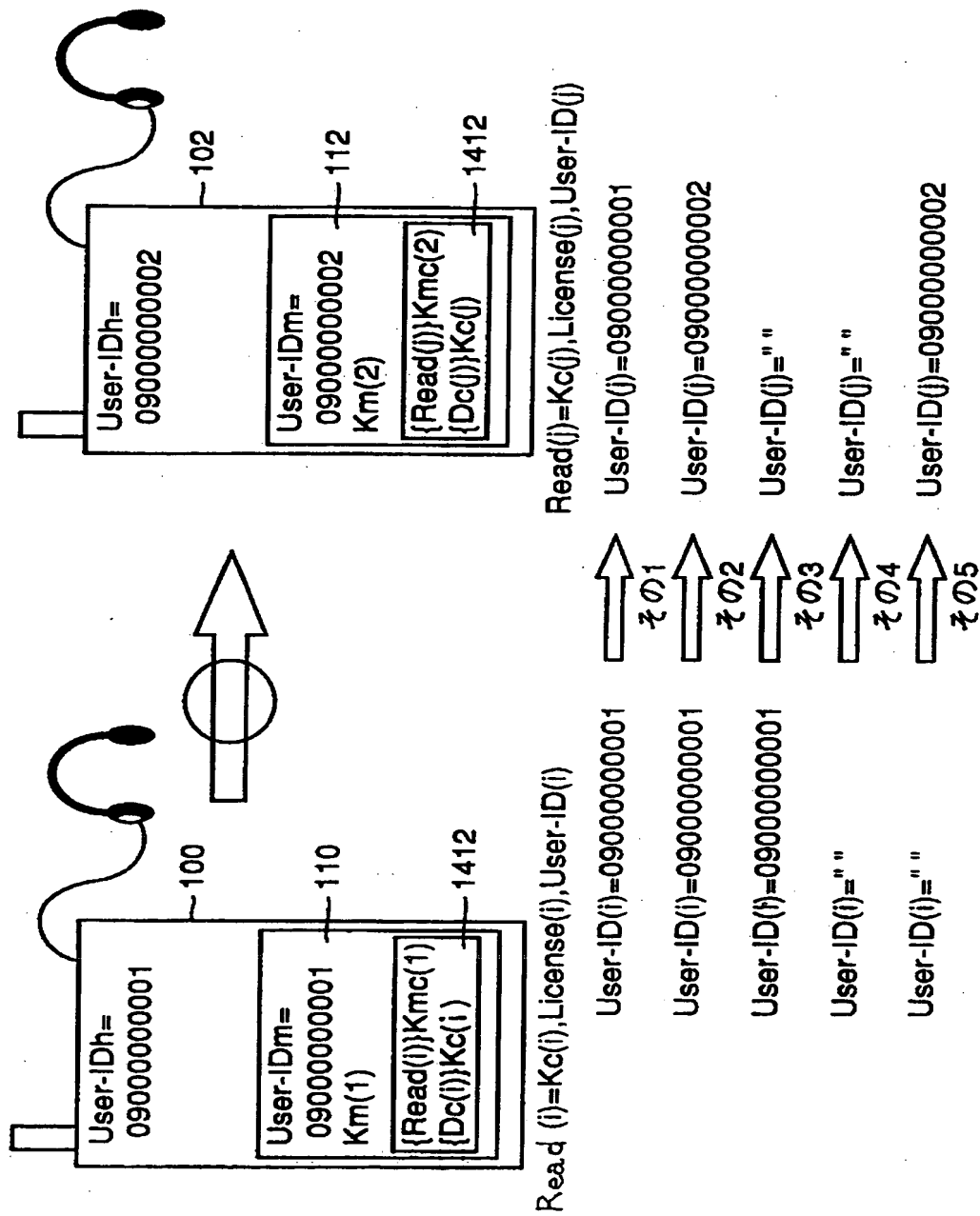


【図 1 7】

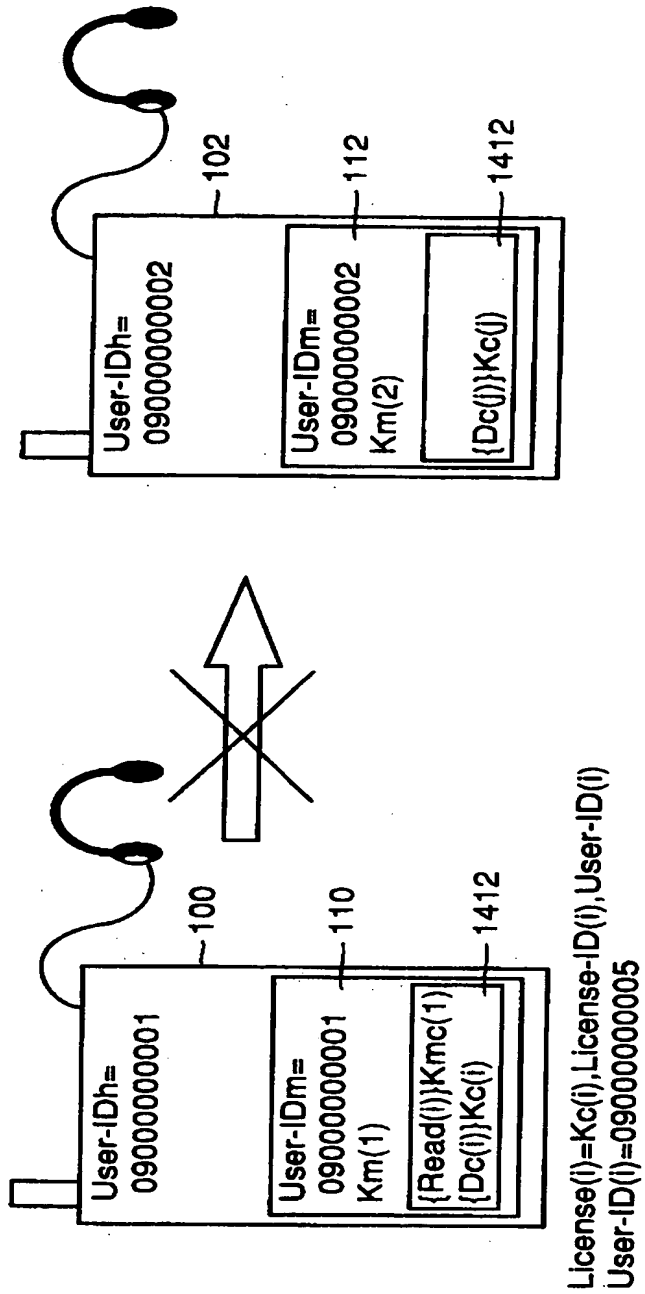
移動



【図 1 8】



【図 1 9】



【書類名】 要約書

【要約】

【課題】 ユーザの許可なく配信データを消去、移動されることを防止することが可能な記録装置を提供する。

【解決手段】 メモリカード 1 1 0 は、メモリカードのユーザを識別するユーザ ID データを保持するユーザ ID 保持部 1 5 3 0 と、メモリカード 1 1 0 に対するアクセスを制限する第 1 の保守情報を保持する第 1 の保守情報保持部 1 5 2 0 と、コンテンツデータごとのアクセスを制限する第 2 の保守情報を保持する第 2 の保守情報保持部 1 5 4 0 とを備える。メモリカード 1 1 0 は、ユーザ ID データに基づいて、再生装置側のユーザを識別し、正規なユーザ以外が第 1 および第 2 の保守情報を変更することを禁じる。

【選択図】 図 2

認定・付加情報

特許出願の番号	平成11年 特許願 第243741号
受付番号	59900838651
書類名	特許願
担当官	濱谷 よし子 1614
作成日	平成11年 9月 3日

<認定情報・付加情報>

【特許出願人】

【識別番号】	000005223
【住所又は居所】	神奈川県川崎市中原区上小田中4丁目1番1号
【氏名又は名称】	富士通株式会社

【特許出願人】

【識別番号】	000005108
【住所又は居所】	東京都千代田区神田駿河台四丁目6番地
【氏名又は名称】	株式会社日立製作所

【特許出願人】

【識別番号】	000004167
【住所又は居所】	東京都港区赤坂4丁目14番14号
【氏名又は名称】	日本コロムビア株式会社

【特許出願人】

【識別番号】	000001889
【住所又は居所】	大阪府守口市京阪本通2丁目5番5号
【氏名又は名称】	三洋電機株式会社

【代理人】

【識別番号】	100064746
【住所又は居所】	大阪府大阪市北区南森町2丁目1番29号 住友 銀行南森町ビル 深見特許事務所
【氏名又は名称】	深見 久郎

【選任した代理人】

【識別番号】	100085132
【住所又は居所】	大阪府大阪市北区南森町2丁目1番29号 住友 銀行南森町ビル 深見特許事務所
【氏名又は名称】	森田 俊雄

【選任した代理人】

【識別番号】	100091409
--------	-----------

次頁有

認定・付加情報（続き）

【住所又は居所】	大阪府大阪市北区南森町2-1-29	住友銀行 南森町ビル 深見特許事務所
【氏名又は名称】	伊藤 英彦	
【選任した代理人】		
【識別番号】	100096781	
【住所又は居所】	大阪府大阪市北区南森町2-1-29	住友銀行 南森町ビル 深見特許事務所
【氏名又は名称】	堀井 豊	

出 願 人 履 歴 情 報

識別番号 [000005108]

1. 変更年月日 1990年 8月31日

[変更理由] 新規登録

住 所 東京都千代田区神田駿河台4丁目6番地
氏 名 株式会社日立製作所

出 願 人 履 歴 情 報

識別番号 [000004167]

1. 変更年月日	1990年 8月21日
[変更理由]	新規登録
住 所	東京都港区赤坂4丁目14番14号
氏 名	日本コロムビア株式会社

出 願 人 履 歴 情 報

識別番号 [000001889]

1. 変更年月日	1993年10月20日
[変更理由]	住所変更
住 所	大阪府守口市京阪本通2丁目5番5号
氏 名	三洋電機株式会社

THIS PAGE BLANK (USPTO)

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

THIS PAGE BLANK (USPTO)